A Survey on Security in Wireless Sensor Networks: Attacks and Defense Mechanisms

Ilker Korkmaz
Department of Computer Engineering at Izmir University of Economics, Turkey
Orhan Dagdeviren
International Computer Institute at Ege University, Turkey
Fatih Tekbacak
Department of Computer Engineering at Izmir Institute of Technology, Turkey
Mehmet Emin Dalkilic
International Computer Institute at Ege University, Turkey

ABSTRACT
Wireless sensor network (WSN) is a promising technology that has attracted the interest of the research in the last decade. Security is one of the fundamental issues in sensor networks since sensor nodes are very resource constrained. An attacker may modify, insert and delete new hardware and software components to the system where a single node, a specific part of the sensing area and the whole network may become inoperable. Thus, the design of early attack detection and defense mechanisms must be carefully considered. In this chapter, we survey attacks and their defense mechanisms in WSNs. Attacks are categorized according to the related protocol layer. We also investigate the open research issues and emerging technologies on security in WSNs.

INTRODUCTION
In the last few years, with the advancements in technology, new device designs that are different than the personal computers, laptops and servers have been introduced and used extensively all over the world. These devices are smaller and cheaper, and use less energy than the ordinary designs. Besides, they are designed on the integrated circuits having a low power communication unit. Their design techniques provide the use of wireless sensor networks (WSNs). A microprocessor of a sensor node not only includes volatile memory and processor but also includes non-volatile memory, digital to analog converter, analog to digital converter, universal asynchronous receiver transmitter and interrupt controller interfaces. In addition, low range radio frequency, infra-red and optical communication techniques are used in these nodes. Moreover nodes can sense heat, light, acceleration and chemical contaminants from the environment and can send these information through a wireless communication channel.
WSNs are ad hoc networks that are composed of hundreds to thousands self-organizing sensor nodes. An example WSN is given in Figure 1. Each sensor node may collect information from the sensing area and relay its data to the sink node on a multi-hop path. Sink is a gateway node that collects data from the other nodes located on sensing area and aggregates the delivered data. Sink node may communicate with a repository in order to deliver its collected data. The data repository may store data in various forms in order to give query service to the users through Internet.
WSNs have many application areas in today's world (Garcia-Hernandez, 2007). One of the most important applications is habitat monitoring. In the Great Duck Island (GDI) application, the life cycle of storm petrel birds are monitored by researchers from UCB and Intel (Mainwaring, 2002). In the PODS

application (Biagioni, 2002) developed in Hawaii University, some endangered plant species are investigated. ALERT system is developed for the early detection of flood threat by measuring water level, heat and wind power. Another application area of WSN is patient's health monitoring. Schwiebert (2001) developed a system for blind people to sense the objects in their environment. Remote patient monitoring and management of drug usage are the other type of health-based applications (Akyildiz, 2002). Another WSN application is home and office deployment. Srivastava (2001) developed a kinder garden project for educating children.

An attack on a WSN can be defined as a bad behavior by a single node, malicious invasion on a specific part of the sensing area, or an action to defect the operation of the whole system (Sokullu, 2008). The adversary is used synonymously with the attacker which is the originator of an attack (Wood, 2004). The adversary attacks to the network with the aim of damaging a single or group of nodes in order to gain more selfish benefits on the related services than the other nodes of the WSN (Sokullu, 2009). The attacker may exploit protocol weakness to gain network resources, may create fake packets, may overwhelm the nodes, may behave strangely like switching between on and off status or even may simply reach and reprogram the sensor nodes. The basic feature of these attacks is that they are entirely unpredictable (Radosavac, 2007). Identification and investigation of these attacks are very important to design defense mechanisms or counterattacks.

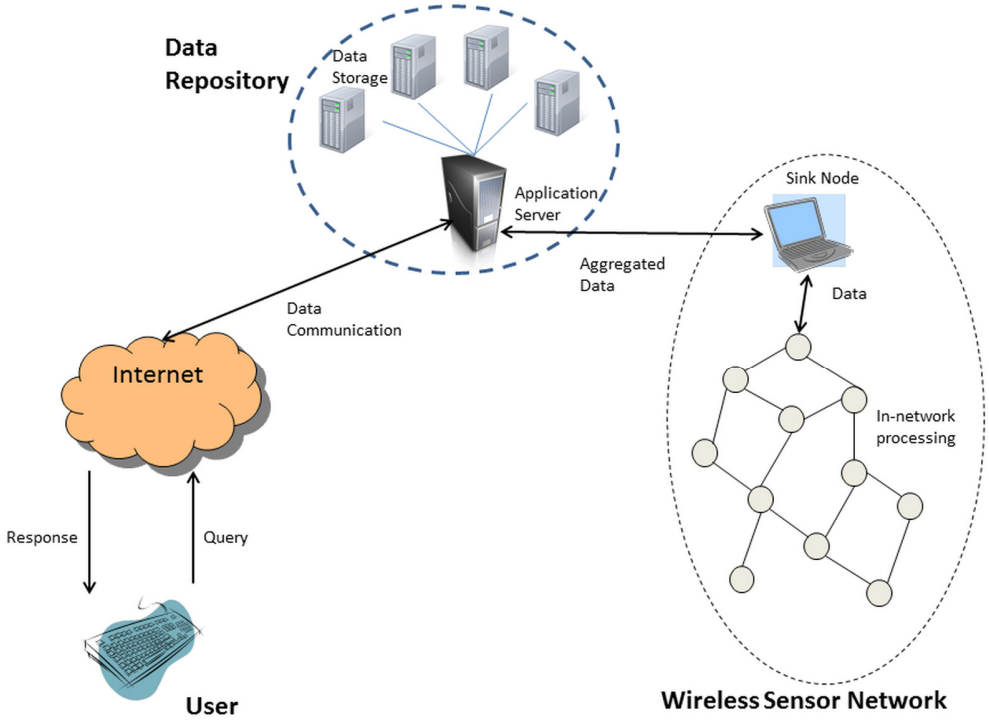

Figure 1. WSN Integrated Information System Example

Today, WSNs in various topologies are used with many different applications that are integrated into kinds of Information Systems. To us, the security of those Information Systems is strongly associated with the security of the WSN used within. For that reason, we believe that a chapter covering the WSN attacks and their defense mechanisms as a detailed survey on the security in WSNs would be properly related to the content of Secure Information Systems.

In this chapter, we classify the WSN attacks by considering the related protocol layers as physical layer, data link layer, routing layer, transport layer and application layer. For each attack, we give its definition,

effects and defense techniques. We also provide the open research issues for WSN attacks as use of privacy homomorphism, overhearing, integrating IPv6 to WSN, emerging wireless sensor and actor network problems. The chapter is organized as follows: The attacks and defense mechanisms are covered in Section ATTACKS AND DEFENSE MECHANISMS, open issues are discussed in Section OPEN ISSUES, and the conclusions are drawn in Section CONCLUSIONS.

ATTACKS AND DEFENSE MECHANISMS

Any possible attack to WSN is a threat for the Information System integrated to the corresponding WSN. As an attack to any part of the hardware or software of the WSN may give a significant damage to the Information System in use, the defense mechanisms to that attack should be taken into consideration at every stage of the system. From this perspective, the possible attacks and defense mechanisms against these attacks need to be discussed and a trade-off analysis of pros and cons for handling the defense mechanisms is also needed to be considered for a compact risk assessment of the used WSN infrastructure.

A view on top of all types of attacks in WSNs, an attack to a WSN may target mainly the followings: i.) the hardware/software of any part of the WSN; ii.) the communication protocol at any part of the WSN. The attackers may directly access to at least one node of the WSN or may give harm to the data communication by interfering with the communication channel or may get into the network without being recognized. From both the point of view of the attacker and the attacked network, the incurred damage is the essential criteria to evaluate the result of the attack. Rather than evaluating the attack results and then comparing the attacks one another, the researchers consider any different attack independently and generally based on a scenario. From this point, the view of the researchers on attacks in WSN literature has been categorized in various ways. In many classifications, the common criterion of the attacks is generally the targeted protocol layer of the sensor network; however there are also some other criteria such as regarding the objectives of the attacks, the security services targeted by the attacks or some hybrid classifications. On this point, Karlof (2002) discusses the attacks to routing layer of WSN and their countermeasures. Sharma (2011) also gives a brief survey of the attacks distressing the routing layer. Chan (2003) makes a categorization for the attacks based on the physical, MAC, and routing layers. As a more general view, Raymond (2008) categorizes the denial of service attacks and defenses by protocol layer taking into consideration all OSI layers, physical, link, network, transport, and application layers. Sokullu (2008), Sokullu (2009) and Lupu (2009) survey the attacks with a classification based on all protocol layers. Sokullu (2008) and Sokullu (2009) also introduce a new attack on MAC protocol layer (defined as GTS attack targeting to the frame structure of IEEE 802.15.4, which is used as a standard MAC protocol for WSN) and explain the different behaviors of the attacker based on different scenarios. Deng (2005) proposes to deal with the attacks aiming the traffic analysis and gives countermeasures to make the base station not to be located easily by such an attack. Padmavathi (2009) gives a classification of WSN security attacks based on their objectives of being passive or active in the sensor network. According to the availability, authentication, integrity, and confidentiality services, the security issues for ad hoc wireless networks are taken into consideration by Stajano (1999). Sen (2009) gives a categorization of the WSN attacks based on the security services and requirements, in addition to this, attacks are also categorized according to their target layers. Yu (2012) describes the trust mechanisms in WSNs and categorizes the trust related attacks in WSNs.

This section mainly gives the state-of-the-art of the attacks and their defense mechanisms in WSNs. The important attacks to WSNs are categorized by their target protocol layers. A general summary of the WSN attack classification according to protocol layers are depicted in Figure 2. As the section surveys probably every known attack in WSN literature, we propose that it is an essential up-to-date reference to the study area of the WSN security literature.

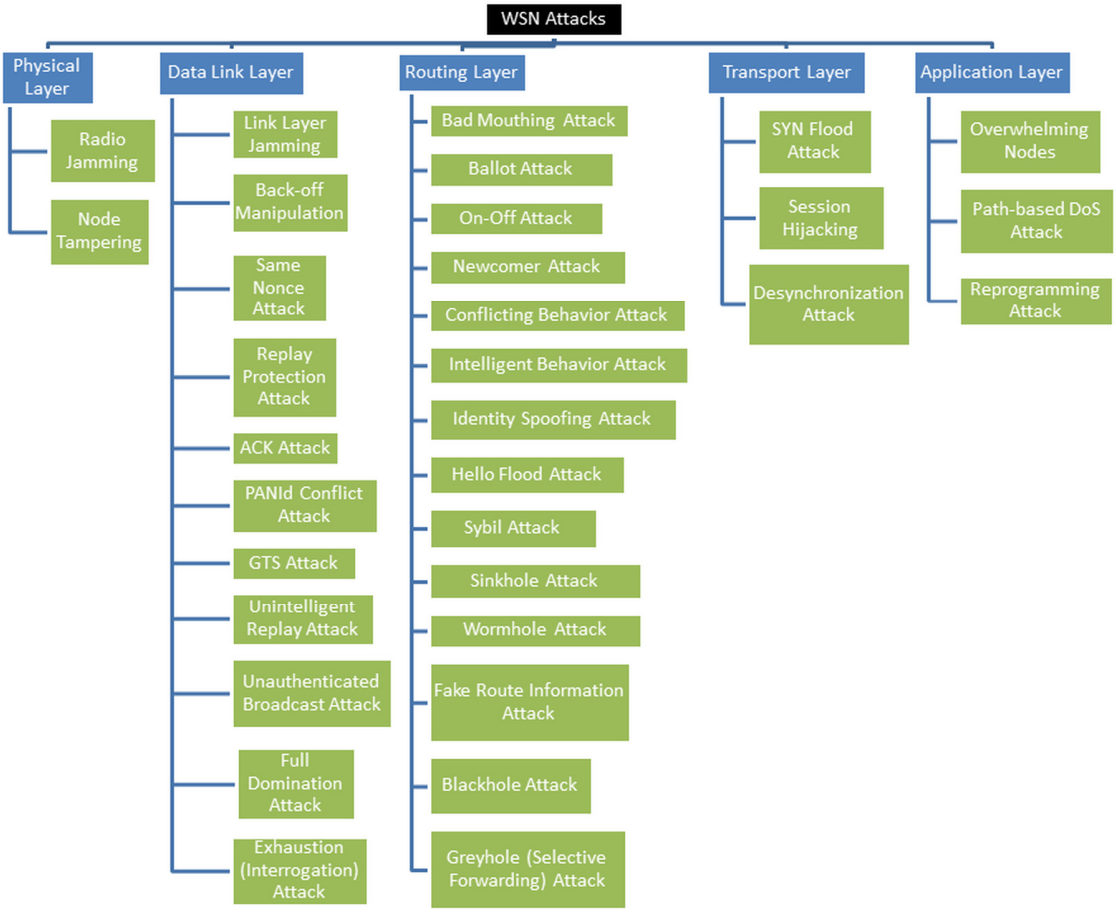

Figure 2. WSN Attack Classification

Physical Layer

Radio Jamming: In this attack, adversary emits just signals to interfere in the communication (Raymond, 2008). Because of this behavior, the attack is simple to implement on any type of sensor network environment. It is very effective since it corrupts the communication channel due to frequency interferences. For example assume that two nodes are communicating to transmit a critical data. At this moment, the adversary can emit signals in order to interfere with the data packet. This leads to corruption of the data packet and retransmission of it causing energy consumption. If the jammer is located at a critical position, the effect of the attack can be more harmful. An example case is depicted in Figure 3 where 7 nodes are forming a sensor network. The transmission range of each node is shown with dashed circles where node is in the center of it. The jammer node is node 7 where it is depicted with black filled style. As seen on the figure, jammer node can affect all the other nodes since they are within transmission range of it.

One of the defense techniques against this attack is implementing spread spectrum communication in radio units of sensor nodes (Raymond, 2008). Although this defense is effective, it is not feasible in many aspects to implement spread spectrum in sensor network radio units. Because of this fact, this defense strategy can be theoretical solution of low cost sensor nodes. The other technique is adjusting the sleep durations by switching from radio on mode to radio off mode. This adjustment can also be implemented by encrypting protocol packets which announce sleep/wake intervals. For example beacon packets in IEEE 802.15.4 includes sleep/wake intervals to synchronize sensor nodes. So these beacon messages can

be encrypted not to inform possible jammers about sleep/wake intervals. This action causes not to receive jamming signals and to protect corruption of data message. Moreover, the adversary redundantly consumes its energy by emitting signals while ordinary nodes are sleeping.

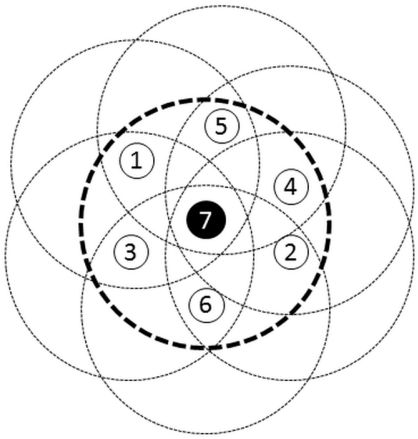

Figure 3. An Example Jammer Located at a Critical Position

Node Tampering: This attack is done by an adversary who can freely enter to the sensing area and can physically handle sensor nodes (Raymond, 2008). In this case, attacker can simply modify the software in sensor nodes in order to disrupt the operation or can install harmful software to make the sensor node as a new adversary. The attacker may also modify or insert new hardware components for the same purposes. Moreover, the adversary may capture private information such as stored event data, cryptographic data, etc.

This attack can be weak when network includes thousands of sensor nodes considering the fact that it is very time consuming for the adversary to reach each node and to modify them. Regarding this, the first defense mechanism to this attack is camouflaging sensor nodes to increase the physical search time of sensor nodes. This defense is very common especially in military applications. On the other hand an intelligent attacker may select critical nodes on data delivery paths to tamper them. In this case a dense deployment of sensor nodes may help to continue data delivery. In addition to these defense mechanisms to prevent data capture, a self-destruction defense mechanism can be implemented on sensor nodes. Furthermore, an encryption mechanism may also be implemented to sensor software in order to protect from software modification. Although this mechanism may not protect node from new software installation, it may prevent easily modification of complicated applications.

Data Link Layer

Link Layer Jamming: In this attack, adversary knows the logics of the link layer protocol and creates collision at the link layer (Law, 2005). The adversary sends link layer packets at data transmission time of the target nodes. By this action, the adversary misinterprets the channel use rules to prevent the legitimate users from accessing to the medium. In contrast to blind attacks in radio jamming, link layer jamming is an intelligent and energy efficient attack that aims to attack at planned times to preserve the energy of the adversary.

In most of the link layer protocols, message schedule is shared by sensor nodes before beginning synchronous data transmission. This provides a common schedule for the nodes involved in data transmission. Although this technique can be useful for communication, it can also cause to leak schedule information to adversary nodes. Thus the first defense mechanism is the encryption of each packet including scheduling information. If single key is used for encryption, then it may be vulnerable to key stealing. If keys are generated between nodes, then energy consumption may be very high. The second

defense mechanism is data blurting or schedule switching. In this technique, when a node cannot receive ACK packet from its destination, it changes the communication schedule and announces (Law, 2005). Law (2005) simulated the implementation of this attack together with an appropriate countermeasure in OMNeT++ platform. OMNeT++ is a modular object oriented discrete event network simulator (OMNeT++, 2012). In the attack simulation, 100 nodes are randomly dispersed in test area. These nodes use S-MAC protocol with a duty cycle of 10% at the link layer, TinyDiffusion at the network layer and run TinyOS as the operating system.

Back-off Manipulation: Many data link layer protocol includes a back-off timer to prevent more than one node to access medium at the same time. Back-off timers are usually designed to sleep for randomly chosen times. A node can selfishly choose a small back-off interval in order to sleep less and gain unfair access to the medium (Radosavac, 2007). Famous CSMA-CA based protocols such as IEEE 802.11 and IEEE 802.15.4 are prone to this attack.
This attack is hard to detect in nature because attacker's behavior is hard to be characterized. Attacker can choose any integer for back-off timer, thus it can communicate with the other nodes at any time it wants. A defense mechanism is to check attacker whether it uses truly random numbers for exponential back-off timer (Radosavac, 2007). This mechanism can be executed by an ordinary monitoring node. This defense mechanism is implemented with OPNET simulator which is a high level event based network simulator (OPNET, 2012). Another defense strategy can be encryption of back-off mechanism related protocol packets; the encryption might not permit selfish attacker to choose small back-off intervals.

Same Nonce Attack: Sensor nodes may store an access control list (ACL) which has the list of nodes for communication. Each ACL entry has a destination address, the key, the nonce, and option fields. These fields are used in an encrypted message communication. If the same key and nonce pairs are used within two transmissions, an adversary who obtains those ciphertexts may retrieve useful information (Xiao, 2005).
Same nonce can be occurred in many situations such as sleep mode, power failure, hardware malfunction, etc. Besides, same keys can be occurred when situations such as using broadcasting keys and grouping keys. The defense mechanism to same nonce attack is firstly to add new fields to the message such that separating nonce field from the frame counter (Xiao, 2005), so two fields are both used at the same time. The security of the message is enhanced in this case, but an additional field transmission overhead will be added to the system. The other defense mechanisms are to use timestamp instead of frame counter and dynamically dividing nonce spaces such that different entries with the same key will use different space of nonce values. Xiao (2005) proposed separating nonce field from the field counter and using timestamp instead of frame counter techniques for IEEE 802.15.4 based sensor networks. Nevertheless, these proposed methodologies are explained without their real implementations.

Replay Protection Attack: Replay protection mechanism in IEEE 802.15.4 is used to accept a frame by checking if the counter of the recent message is larger than the previous message. An adversary in a sensor network may target this replay protection mechanism (Xiao, 2005). For example an adversary sends many frames with large counters to an ordinary sensor node. After this attack, the ordinary sensor node will reject the legitimate frames with small counters from other legitimate nodes.
In IEEE 802.15.4, to prevent replay protection attack the frame counter is used. As mentioned in same-nonce attack, the frame counter may cause problems in some situations. To provide sequential freshness, the defense mechanism is to use timestamp instead of frame counter as also mentioned in same-nonce attack. With this mechanism, there will not be a replay counter to be incremented. The drawback of this approach is the increasing message size. Besides a time-synchronization mechanism should be provided. Although there are not given any specific implementation details of these mechanisms, the methodologies of the approaches are noted in (Xiao, 2005).

ACK Attack: Assume a channel is used by two parties where first node sends a data packet, the other node replies with an ACK packet after successful reception of the data packet. In ACK attack, an adversary should firstly eavesdrop the channel of communicating two parties (Xiao, 2005). Then the adversary should block the data packet of the first node to prevent successful packet transmission. Lastly, the adversary generates a fake ACK packet as generated from the first node, and sends this packet to the second node.
ACK frames do not have any integrity protection mechanism. In order to provide this mechanism, message integrity code (MIC) can be appended at the end of the ACK frame (Xiao, 2005). MIC can be obtained by AES-CBC-MAC authentication algorithm provided in IEEE 802.15.4 security suites where whole ACK frame can be used as the authentication field. As replay protection and same nonce attacks, no specific implementation of the countermeasure for ACK attack is given in any specific format.

PANId Conflict Attack: A PANId conflict occurs in a personal area network (PAN) if there exists more than one PAN coordinator operation in same personal operating system (POS). PANId conflict attack is created by creating fake conflict messages within a PAN (Sokullu, 2007). In this attack, an adversary may send fake PANId conflict notification messages to overwhelm the PANId coordinator. After PANId coordinator receives PANId conflict notification messages, PAN coordinator executes conflict resolution procedure that prevents the data transmission between PAN coordinator and legitimate nodes at the same time.
In order to defend PANId conflict attack, the coordinator my simply check two parameters: the conflict count for any node and the maximum conflict count in a deterministic time interval (Sokullu, 2007). If PAN coordinator detects the attacker, it can ignore any packets originating from the adversary node. These rules can be integrated to IEEE 802.15.4 MAC layer protocol. The implementation details of this attack and its defense mechanisms are set up in version 2.34 of ns2 platform, which is a discrete event simulator and developed at ISI, California (Ns2, 2012). Single attacker, double attacker and triple attacker scenarios are implemented within a fixed size star topology with the fixed coordinator parameters.

GTS Attack: PAN coordinator can assign dedicated slots to network devices in IEEE 802.15.4 standards. Guaranteed time slot (GTS) is a slot assigned by the coordinator to a device to warrant collision free transmission. The applications with predefined bandwidth requirements can be supported by GTS based communication. In GTS attack, the adversary may disrupt the communication between a device and its PAN coordinator (Sokullu, 2009). The attacker first synchronizes with the PAN coordinator by receiving beacon messages. At the same time attacker may learn the GTS times of the legitimate nodes. To accomplish the GTS attack, the adversary sends data packets at GTS moments in order to create interference and collision. Sequence diagram of this attack is given in Figure 4.

GTS attack is hard to detect and defend. Since the adversary synchronizes its time with the PAN coordinator, the attacker creates collision at exact GTS moments where it is hard to detect by PAN coordinator. In this case, the PAN coordinator cannot perceive the ID of the attacker. On the other hand, if attacker and PAN coordinator do not synchronize in a fine-grained way, the coordinator may detect the attack and extract the ID of the adversary (Sokullu, 2009). But this case is also unrealistic since an intelligent attacker may hide its ID from packets. To derive a defense solution to this attack, we can firstly characterize the basic nature of the GTS attack. In GTS attack, the communication between two legitimate nodes is corrupted by an intelligent and synchronized attacker. From this fact, we may state that attacker behaves like an intelligent jammer. So that some defense mechanisms which are covered for jamming can be applied to GTS attack. For example, although it is an expensive solution, different frequencies can be assigned to each node by PAN coordinator for GTS transmission. In this case, adversary should learn frequencies of each transmission. Besides that, the GTS fields in beacon message can be removed not to leak information to adversary. To support this operation, protocol rules should be reorganized. Finally, GTS request messages can be encrypted in order to prevent information leak to the attacker. This encryption technique can be chosen as asymmetric key cryptography if total node count in a

PAN is small. In this small sized star topology case, memory allocation for public keys will not be a problem. Conversely, symmetric key cryptography will probably be more suitable for large scale sensor networks. As a popular implementation tool for the use of symmetric key cryptography in sensor networks, SPINS (Perrig, 2004) can be chosen since it provides broadcast authentication, two-party authentication, data confidentiality and integrity. We think that using SPINS in the countermeasure implementation of GTS attack is appropriate because the focus point of the defense involves the communication with base station (PAN coordinator).

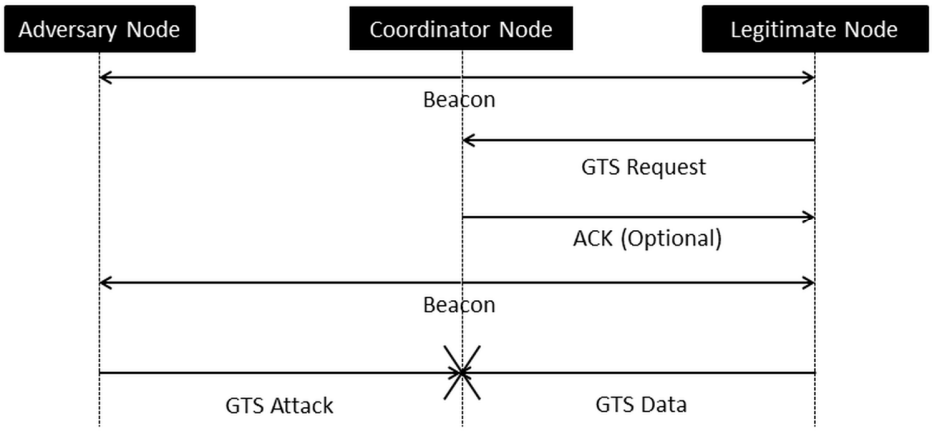

Figure 4. GTS Attack Sequence Diagram

Unintelligent Replay Attack: In this attack type, the attacker sends recorded events into the network in order to prevent nodes from entering to the sleeping state, thus the adversary causes significant energy consumption (Pawar, 2012). If sensor nodes do not have anti-replay mechanism, the previously sent data messages are redelivered into the network. Because of this operation, network-wide energy consumption increases. This attack causes both local and global waste of energy.
The defense mechanism is the anti-replay protection technique. In this technique, sequence numbers are tracked as packets arrive. As mentioned previously in replay protection attack, timestamps may be used instead of sequence numbers to provide sequential freshness.

Unauthenticated Broadcast Attack: The adversary knows MAC rules in this attack, but cannot penetrate the network (Pawar, 2012). The attacker follows the MAC rules and broadcasts unauthenticated traffic into the network. These packets consume the energy of nodes in two ways: Energy consumption from radio transmission and energy consumption from decreasing sleeping period. This energy consumption reduces the network lifetime. To defense this attack, schedule switching and spread spectrum communication may be used. Another idea as a general defense solution is using encryption. Protocol packets can be encrypted in order to prevent leaking of schedule information from legitimate nodes. However, encrypting all packets adds so much extra cost to the whole system. An indirect solution, which mainly changes the context of this attack and the view of the communication to the attacker, may be to use authentication in only broadcast messages. Authenticated broadcast problem have been attractive for the sensor network researchers and its more energy constrained implementation may still be seen as an open issue. A very popular implementation tool for the authentication for data broadcast in sensor networks is μTesla, which is one of the main secure components of SPINS (Perrig, 2004).

Full Domination Attack: The adversary knows MAC rules in this attack and can penetrate the network in contrast to unauthenticated broadcast attack (Pawar, 2012). The attacker follows the MAC rules and produces trusted traffic to gain maximum benefit. This attack is very dangerous since attacker

intelligently uses all protocol rules in a selfish manner. One or more attacker nodes can participate in full domination attack. The defense mechanism for full domination attack is not unique and depends on the attack type. For example, similar to defense mechanism of unauthenticated broadcast attack, protocol packets can be encrypted not to leak information to attacker.

Exhaustion (Interrogation) Attack: The exhaustion attacks are applicable on WSN when nodes use MAC protocols based on request to send (RTS) and clear to send (CTS) packet exchanges. In this type of MAC protocol, a sender node initiates the data transmission by sending a RTS packet. The receiver node receives RTS packet and replies with a CTS packet. Any other node receiving RTS and CTS messages cannot send data and waits for a period of time. This approach solves the hidden node problem in wireless ad hoc networks. In this attack, the adversary node sends RTS packets repeatedly (Raymond, 2008). The RTS receiver node replies with CTS packets repeatedly causing energy consumption and exhaustion of its battery.
The defense mechanism for this attack can be similar with PANId conflict attack's defense mechanism. The receiver node my check the RTS count and maximum RTS count in order to defend exhaustion attack. If receiver node finds that RTS count exceeds maximum RTS count, it decides sender node is an attacker and it can ignore any packets originating from that adversary. Since RTS and CTS packets are small in size, using an encryption will not be a convenient countermeasure suggestion for this attack.

Routing Layer

Trust Related Attacks and Defense Mechanisms

Reputation is simply the idea about trustworthiness of an entity about another entity. Historical knowledge affects the entity to have positive, negative or neutral thought for the intended element. In daily life, people make good connections with whom they have good reputations about. The amount of reputation implies having a trust level about the related person (or entity). Thus, reputation may be concerned as input to calculate trust values. The main notion is to obtain trust values according to trustworthiness of individual nodes by using the collaborative behavioral messages from related node's neighbors (Sun, 2008). So the trust value about a node helps giving a decision to interact with it. In accordance with defense mechanism, nodes with low trust values may be suspected to misbehave.
In WSNs, nodes can produce reputation about other nodes. The increasing positive reputation about a trusted node helps determining a goal as forwarding packets through other nodes in WSN. In a reputation and trust-based system, reputation is recorded and utilized to create trust information where trust affects nodes how to act in the network (Srinivasan, 2008).
In trust-based systems, sensor nodes should be initialized to get starting reputation values. There are three initialization choices for sensor nodes. Firstly, every sensor node can be considered as a trusted node and they trust each other (initially positively reputed nodes). When nodes act in WSN, the reputation of nodes decrease and they can be untrusted by time. Secondly, every sensor node can be considered as an untrusted node and they do not trust each other (initially negatively reputed nodes). When they behave positively their reputation will increase. As the last approach, all nodes are supposed to have neutral reputation (initially neutrally reputed nodes). The interaction of nodes helps them to increase or decrease their reputation values (Srinivasan, 2008).
Sensor nodes can update their reputation with first-hand or second-hand observation. In first-hand observation, nodes directly sense the state changes and update reputation without external effect (direct trust). However, direct trust is calculated by the value of successful interactions between subject node and interacted node. There is a special kind of direct trust named as recommendation trust. Recommendation trust considers direct observations and the recommended nodes from its neighbors. Subject node compares the reputations (good or bad recommendations) supplied by its neighbors with first-hand observations and calculates a trust value. In second-hand observation, subject node tries to discover the trustworthy collaborative nodes to achieve its goal. Therefore, subject node requires the information of

neighbor nodes to update its local data (indirect trust). If neighbor nodes send recommendations (positive reputation) about a third node to subject node, indirect trust is provided by trust propagation (Sun, 2008).
In distributed multicast networks, secure authentication and authorization are crucial issues if the members of a multicast group change frequently. To be used in such multicast ad hoc networks, Chang (2008) proposed a two-step secure authentication approach. In the first level, the trust value of each one-hop neighbor is calculated by a Markov chain trust model. In the second level, a node with the highest trust value of a group is chosen and it is labeled as central authentication (CA) server. For reliability issues, node with second highest trust value is selected as backup CA server and secure authentication for group management is formed via trust.
Trust mechanisms look promising in terms of strategic defense approaches. However, there are also trust related attacks at routing layer and the explained followings are some popular ones.

Bad Mouthing Attack: Adversaries supply negative reputation of compromised sensor nodes to the neighboring nodes. The negative reputation from adversaries makes trustworthy sensors calculate the trust value of compromised node negatively (Pathan, 2010). In a WSN including positively or neutrally initialized nodes with second-hand information, sensors can share negative feedback to neighboring nodes and bad mouthing attack may be appeared.
By the viewpoint of subject node, historical recommendations acquired by that node are used for defense mechanism. However, trust is taken into account by good or bad recommendations. In defense mechanism of bad mouthing attack, malicious nodes may be detected using malicious node detection performance metric (Sun, 2008). Each node detects the malicious interacted node locally using average detection rate (AVD) and false alarm rate parameters. AVD is calculated dividing total number of nodes in good behavior, which detect malicious nodes, by the set of malicious nodes. False alarm rate is calculated similarly to AVD except changing denominator with the set of good nodes. Sun (2008) shows that recommendation trust approach increases the detection rate of attacks with malicious node detection performance metric. There is a threshold value for trust recommendation which affects trust propagation. If threshold passes a predefined value between two neighbor nodes (A-B) for a trusted path (A-B-C), trust propagation is permitted for the third node from its neighbor (B-C).

Ballot Attack: Ballot attack is the opposite of bad mouthing attack according to adversary's behavior (Pathan, 2010). Adversary supplies positive reputation of compromised nodes to their neighboring nodes. Adversary forwards reputation of malicious or badly reputed nodes to trustworthy nodes positively. In a WSN including negatively or neutrally initialized nodes with second-hand information, nodes can share positive feedback to neighboring nodes and ballot attack may be appeared.
The defense mechanism explained for bad mouthing attack may also be used similarly for ballot attack.

On-Off Attack: In this attack type, adversary behaves in nondeterministic manners not to be detected by the other nodes in WSN (Sun, 2008). Adversary sends alternatively positive and negative reputation values to neighbors. So its misbehavior cannot be detected easily and negative reputation values can be distributed to WSN for a long time before detection. The trust value for the adversary node may dynamically change.
As a countermeasure, the trust value should be weighted during a timeline using a parameter named as forgetting factor. Forgetting factor is based on observing the good actions for different time intervals. On-Off attack's defense mechanism uses the social life rules. Being a trustable entity takes a long time while decreasing that reliability happens in a short period. Therefore, forgetting factor should be defined adaptively for the periods of good and bad behaviors (adaptive forgetting scheme) (Sun, 2008).

Newcomer Attack: In initially positive or neutral reputed node manner, reputation of adversaries decreases by time with their hazardous behavior to other nodes. Thus they may not attend routing links and act as a passive entity in the network. To erase its bad reputation and perform actively, adversary may rejoin the network as a newcomer and starts functioning with an initial reputation. Attack of reentering the network

with a new ID is also called as whitewasher attack (Lopez, 2010). Attacker may also impersonate or compromise nodes to erase its bad history to be known as a trusted node. If adversary is able to reenter the system repeatedly, detection of untrusted nodes becomes meaningless and defense mechanism in the system should be redesigned.
Authentication and access control are the main concerns to defend against newcomer attack. Therefore new nodes may not reenter continuously to the network by getting new IDs. As another approach, if newcomers have initially negative reputation values and have to behave positively for a long time, this may help decreasing their attacking behavior. Lastly, "pay their dues" approach for a node is based on supplying more service than it receives (Hoffman, 2009). So adversary node should continually behave positively to stay its trust value high for obtaining the service that it needs to acquire.
As a tool to be used for protecting the nodes against bad mouthing and newcomer attacks, a trust evaluation scheme is simulated for mobile ad hoc networks (MANETs) on a self-organized virtual trust network (Misaghi, 2012). To disseminate the trust information through nodes, each node periodically exchanges its trust network with its neighbors. Each node creates a virtual layer to keep trust information of other networks. That information should be obtained by direct or indirect trust approaches. Trustworthiness for the network of the node is computed locally. Performance and effectiveness of the scheme is evaluated with ns2 (Ns2, 2012). The simulation environment covers 100 trustworthy and malicious nodes using IEEE 802.11 with distributed coordination function (DCF) as MAC protocol. For bad mouthing attack and newcomer attack, the scheme may resist up to 10% attackers of whole nodes.

Conflicting Behavior Attack: Adversary behaves differently to different group of nodes. So different nodes have different reputations for the attacker and inconsistent trust values between different groups of nodes occur. While on-off attack is concerned on the unnoticed misbehaviors in time domain, conflicting behavior attack determines the inconsistent behavior in node domain (Yu, 2012). Figure 5 shows a conflicting behavior attack scenario. Node A behaves good to Node C and forwards the packets coming from C. However, Node A misbehaves to Node B and does not forward its packets. When Node B and Node C share their reputations about Node A, there will be conflict on their values and they will not trust each other anymore.

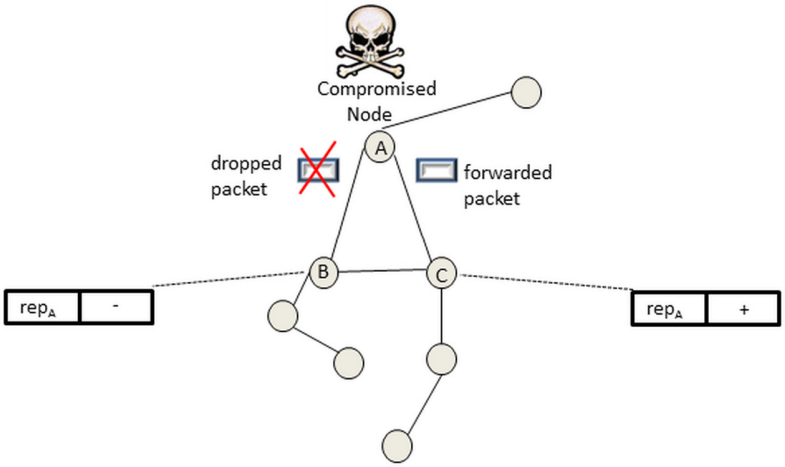

Figure 5. A Sample Scenario for Conflicting Behavior Attack

In this attack mechanism, the adversary node drops the packets of a group of nodes (G_{Nd}) and routes packets of another group of nodes (G_{Nr}) successfully. Attack percentage is defined by the division of G_{Nd} to total number of nodes (Sun, 2008). If attack percentage is low, honest recommendations of attacker

make it a trustable node. If it keeps its honesty for a period of time, attacker detection will be difficult. If attack percentage is high and malicious node continues sending bad recommendations to its neighbors, attacker can be easily detected. If attacker does not want to be detected easily in the network, it does not interact in the network intensely.

Intelligent Behavior Attack: Attacker tries to detect the important information like reputation values or trust ranking in the messages and it adapts its behavior according to that information (Yu, 2012).
To defend against this attack, messages may be encrypted and just the destination node may be permitted to read the content of the message. Thus, the nodes whose goal is forwarding messages may not be aware of the data inside the message and the attacker may not impair the network as long as it does not compromise destination node.

Other Routing Attacks and Defense Mechanisms

Identity Spoofing Attack: In identity spoofing attack, an adversary may capture sensor nodes, replicate them and put them to planned locations in network (Parno, 2005). This may cause disconnection of the network topology and routing cycles. As countermeasures to identity spoofing attack, two distributed techniques can be used (Parno, 2005). In randomized multicast technique, node location information is distributed to randomly-selected witnesses, to exploit the birthday paradox. The other technique is line-selected multicast where topology of the network is used to select witnesses for a node's location and to detect identity spoofed nodes.

HELLO Flood Attack: In some routing protocols of WSNs, announcing the node to its neighbors is realized by broadcasting HELLO packets. Therefore, the sensors which receive radio message from the broadcaster node will assume that node as a neighbor. In reality, adversary node may have a large transmission power to convince the nodes to use itself as a routing node. If the base station is compromised by the adversary, convinced nodes of WSN will send their packets to a geographically further located adversary and the whole network may be in a complicated state (Singh, 2010).
A defense mechanism against HELLO flood attacks is defined as multi-path routing to multi-base stations (Hamid, 2006). In this approach, node authentication is used between regular nodes and multiple base stations. All of the base stations are assigned with the specific keys shared by the ordinary nodes. According to Karlof (2002), a bidirectional link between nodes should be constructed to verify the message traffic. Therefore messages may just be forwarded through this link. A trustworthy sink node defines limitations for verified neighbors of each node to control a large network configuration. Singh (2010) also proposed a detection and prevention method for HELLO flood attack. Nodes that have known radio range strength classify neighbor nodes as "friend" or "stranger" according to the signal quality. If a node is labeled as stranger, it is tried to be verified by client puzzles. However, the puzzles get more complicated with increasing number of non-replied HELLO messages to verify the suspected node's trustworthiness.

Sybil Attack: Adversary node enters the system with more than one identity by compromising different nodes to increase the probability of being chosen on many routes. Shared keys between nodes enable having more than one identity easier. Although signature generation and verification are beyond the capabilities of sensor nodes, using public key cryptography is suggested to solve this problem.
An approach for defense is as follows: Ordinary nodes share a unique symmetric key with the sink node and those nodes create session keys for confidential communication between neighbor nodes (Karlof, 2002). Sink's goal is to restrict the number of neighbors for a node and an error message is sent when the limit is exceeded. If a node is compromised by an attacker, it just may interact with verified number of neighbors, not the whole network. So the negative effect of the attacker to whole network can be reduced until adversary does not create a wormhole which precipitates a verified neighbor having a virtual neighbor.

Newsome (2004) proposed radio resource testing which assumes that every physical device has a radio that may not use different channels simultaneously for message transfer. The node assigns different channels for each of its neighbors (if there are enough channels) to prove the identity of neighbors. Probabilistically, it broadcasts messages to different channels and listens to the related channel to verify the neighbor. If the node does not have enough channels, it may not cover all the neighbor nodes and Sybil node may affect the network indifferently. At this condition, a random subset of nodes and channels are chosen to listen to the traffic for increasing the probability of adversary node detection.
Lazos (2004) proposed a cryptographic and localization based approach for finding the correct position of the node as long as the locator node is not compromised. Sensor encrypts a nonce with pairwise key and concatenates its ID for each locator and then broadcasts those messages to the network. Since the closest located node replies firstly, sensor can determine its actual location.

Sinkhole Attack: The attacker tries to direct traffic through a compromised node. The compromised node convinces the neighbor nodes to route using itself. For example, adversary may persuade sink node by sending a fake quality routing information if sink node does not verify the reliability of the adversary. Furthermore, neighbor nodes will continually use the route that includes compromised node. Those neighbors will inform its neighbors with positive reputation about adversary where the effect of adversary will gradually increase in the network.
Krontiris (2007) proposed an intrusion detection mechanism in which each node has its intrusion detection system (IDS) client. These clients monitor the traffic with the owner node's neighbors. The monitoring process is based on the detection of anomaly behaviors by the rules defined for each node. If anomaly detection is observed by a sensor node, a cooperative mechanism should be enacted for decision of attack with neighboring nodes.

Wormhole Attack: Attackers store the transmitted packets by the legitimate nodes in the network and replays them into the network through the "low-latency out-of-bound" channel (Yu, 2012). Out-of-bound channel, which may not be perceptible by the network, makes detection hard. Wormhole attack is especially harmful at neighborhood discovery phase of a node. Attacker node Y replays the routing request packet of node X to a non-neighbor node Z that causes an unreal neighborhood link.
Karlof (2002) proposed a routing protocol based on the exchange of coordinate information for routing of geographically indicated packets. The packets which are assumed to be forwarded from neighbor nodes may be detected as suspicious if the geographical position information is far from expected. This approach requires the position of node's own location, one-hop neighbors and the location of destination.

Fake Route Information Attack & Blackhole Attack: In fake route information attack, adversary node advertises routing information that the shortest path is routed through itself. Additionally, blackhole attacker drops those received messages.
REWARD is a routing method to obtain a distributed database for the black hole attack in the network (Karakehayov, 2005). This algorithm uses MISS and SAMBA broadcast messages for algorithm utilization. For route discovery, when destination receives a query, it sends its location and waits for new packets. If destination node does not receive a packet in a defined time slot, it sends a MISS broadcast message, which includes the list of the querying nodes' names until that time. The names listed in this message are suspicious nodes which may act as blackhole attackers. Nodes in the network collect those MISS messages and compare the information with their lists to be aware of adversary nodes. On the other hand, SAMBA messages provide suspicious locations of the candidate adversary nodes.

Greyhole (Selective Forwarding) Attack: In this attack, adversary nodes do not forward certain type of messages and drop those packets to prevent dissemination of them anymore. To decrease the suspicion on itself, the attacker selects and modifies the contents of desired packets while others are forwarded unchanged.

If the compromised node is located near the sink node, it may attend data flow directly. According to Karlof (2002), multipath routing is a defense mechanism for this attack. A probabilistic protection mechanism is designed for protection using n different routes that include disjoint nodes even if more than n compromised nodes exist in the network.

Transport Layer

SYN Flood Attack: SYN flood is a kind of denial of service (DoS) attack that attacker creates huge number of half-opened (uncompleted handshaking) TCP connections with a node. A sample sequence diagram for this attack is drawn in Figure 6. Three way handshaking is used to prove that two nodes are ready to make a TCP communication. For this attack, handshaking process never ends between the adversary and the chosen node which means ACK message does not reach to victim node. Adversary learns the return addresses obtained from SYN-ACK packets replied to large number of SYN packets. Victim node starts waiting for beginning the connection by getting the adversary node's message although it will never come. The nodes store the connection requests in a limited size buffer and the buffer will overflow after some number of unsuccessful connection attempts. Therefore, victim node may not accept any more valid connections.

The defense mechanism for this attack is SYN cookies technique. With this technique, connection requests are not kept in target side and the buffer overflow of victim node may be prevented. Responder encodes the SYN message's information and sends it back to requestor to give the responsibility of holding the state (Raymond, 2008).

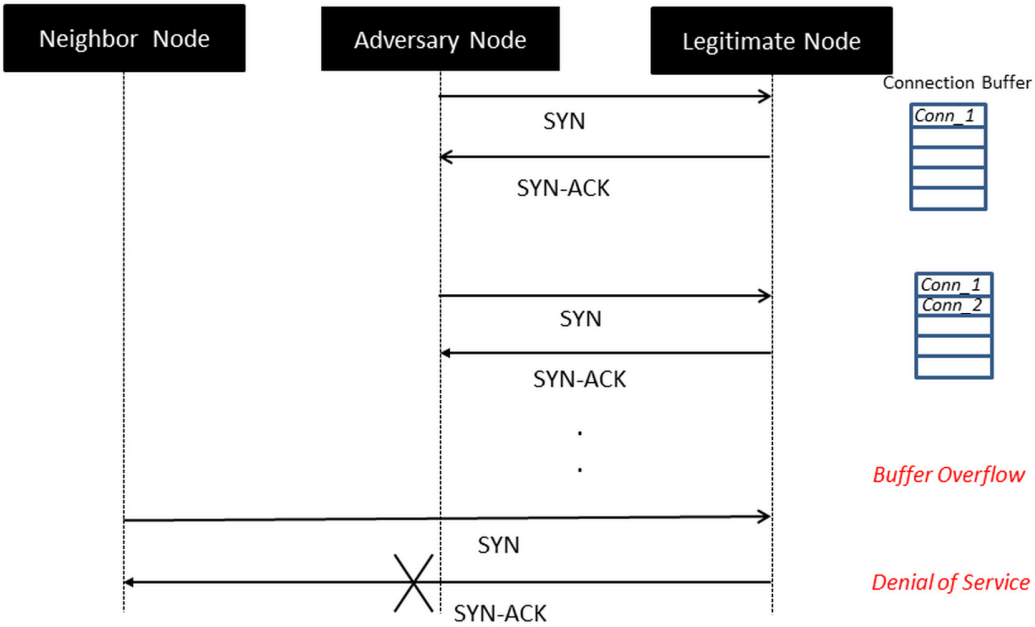

Figure 6. SYN Flood Attack Sequence Diagram

Session Hijacking: Adversary node captures the session information between victim and target. Adversary spoofs the victim's IP address and the message sequence numbers. Then it may continue session with sending correct sequence numbered messages to target with acting as regularly communicated node. Therefore victim node may not be aware of the interruption of session.

Although the usual sensor networks are not based on the use of sessions, in the context of studying the use of IP-based sensor networks, this attack may be a threat. A kind of lightweight protocol providing the secure socket layer (SSL) services may be used as a defense approach. Jung (2009) performed such a

protocol for IP-WSN regarding key exchange, authentication and data encryption on their developed sensor node hardware.

Desynchronization Attack: Attacker interrupts an active connection and sends fake sequence numbered messages to connected nodes. Then the synchronization of message is disrupted and the nodes start retransmitting packets. Authentication of headers or full packets may prevent desynchronization attack (Raymond, 2008).

Application Layer

Overwhelming Sensor Nodes: An adversary node may generate application messages to overwhelm sensor nodes (Raymond, 2008). By applying this attack, network bandwidth is decreased, energy consumption is increased and lifetime of the network is reduced. The adversary can realize this attack if the application is dynamic in nature. For example target tracking application is a dynamic application that uses motion detection mechanism. In contrast to target tracking, a periodical heat measurement application is static and it is not suitable for overwhelming the sensor nodes attack. To defend this attack, efficient data aggregation algorithms can be used (Raymond, 2008). The aim of this defense technique is to reduce the message count disseminated into the network. Encryption of application layer packets can also be a solution for especially new comer attackers.

Path-based DoS Attack: In this attack type, an adversary leaf node injects replayed application messages into the network (Raymond, 2008). This causes forwarding of these messages along the path to the sink node. Hence, the total energy of the network is consumed and network lifetime is reduced. Besides bandwidth for legitimate traffic can be reduced because the attack causes resource consumption on the path to the sink node. The defense mechanisms of path-based DoS attack are packet authentication and anti-replay protection. An alternative method can be packet encryption.

Reprogramming Attack: Sensor nodes can be remotely reprogrammed by protocols such as TinyOS's Deluge (Raymond, 2008). Considering the fact that many sensor network applications are operating on harsh conditions, remotely reprogramming is reasonable. But most of the systems are assumed to be running on trustworthy environments. This brings vulnerability that systems can be reprogrammed by hijackers where large portions of the networks can be controlled by the attackers. In this case, attacker can reprogram the sensor node to take maximum benefit from the application. The defense mechanism of this attack is using authentication streams for reprogramming. Similar to defense mechanism for node tampering, an encryption mechanism may be implemented to sensor software in order to protect it from reprogramming.

OPEN ISSUES

This section discusses the open research issues in the WSN security. Actually, there may be various suggestions on many subjects for directing the researchers to WSN security area. For example, any effort to propose a different countermeasure technique on any attack described in Section ATTACKS AND DEFENSE MECHANISMS would be valuable and appreciated by the academia and industry as well. The motivation on searching for a new countermeasure proposal may be as the following: To propose a defense mechanism which brings up at least the same level of security but consumes at most the same amount of energy than that of an existing one. The pros and cons of the defense mechanism, the cost and benefit on securing the system against the corresponding attack should be taken into account at the beginning. In addition, it needs to prepare a well designed timing schedule whether studying and searching for a new defense mechanism is worth or not. If the study time consumed is too long, different communication protocols or mechanisms may be developed meanwhile and the subject of concerned attack may not be a matter then. On the other hand, we explicitly want to mention that studying on the new attacks, defense mechanisms, or counter attacks in WSN is always an open research area since the

security of Information Systems is strongly related to the security of the WSN used within. In addition, to study on the alternative trust mechanisms to prevent WSN from any trust related attacks would also be valuable.
Yet another advising section, we prefer to take a general top level view on the security issues in the WSNs. Rather than searching for a specific countermeasure against a specific attack in a WSN, we suggest the WSN security researchers to work for a general approach to secure the whole sensor network infrastructure that will provide a secure communication service in the network. It is worth spending effort to the theoretical and practical studies that may come up with solutions to any security issues in WSN. On this motivation, we focus on the general view approaches and defense mechanisms for the communication in the network that seem promising for the future of sensor networks to be used practical and secure within the Information Systems.

Privacy Homomorphism

The fundamental security services that should be provided in any type of Networked Information Systems which are based on the data distribution over wired and/or wireless communication channels are mainly the followings: confidentiality, integrity, authentication, and freshness. Perrig (2002) emphasizes those services as to be the first requirements of sensor network security. Perrig (2004) notes that secure data aggregation is also a network security service for WSN. Data aggregation is mainly the technique for aggregating the logically same data in physically different data packets to reduce the number of total packets delivered within the network to the sink node. Data aggregation term is also used where in-network processing of data is concerned and when the result of gathered data from the sensor nodes is computed at sink as well. On this point, if end-to-end data confidentiality and data aggregation are to be offered in a sensor network, privacy homomorphism (PH) is a promising solution.
PH technique supports a set of restricted mathematical modular arithmetic and so computations can be done on encrypted data. With the help of PH use, any node in the sensor network encrypts the sensed data (confidentiality service) and forwards it to a neighbor node on the path where the sink is targeted to, the forwarding nodes can process and aggregate the received encrypted messages without decrypting (data aggregation via PH method) and sends the new aggregated message in encrypted format. In-network processing through data aggregation is sustained till the sink is reached. Only the sink node decrypts (end-to-end confidentiality service) and recovers the result data in the packet using PH rules. By without decrypting the messages at the intermediary nodes, the total energy of those nodes will be conserved and so the network life time can be prolonged. By reducing the packet number in the network delivered along the sink path, not only the communication bandwidth will be conserved but the total energy consumption to send and receive packets will be decreased as well.
PH is a mathematical base for homomorphic encryption approaches. In a homomorphic encryption scheme that supports data aggregation via PH and so allows modular arithmetic operations on encrypted data, the encryption and the decryption techniques are based on the privacy homomorphic transformations to preserve the privacy. An encryption algorithm E() is homomorphic if given ciphertexts E(x) and E(y), E(x *OPERATOR* y) could be obtained without decrypting them for some operation *OPERATOR*. In this manner, a privacy homomorphic transformation is operatively homomorphic on the ciphertext. If the *OPERATOR* is the addition operator on rings, the transformation scheme is called as additively homomorphic; whereas the transformation is called as multiplicatively homomorphic if the *OPERATOR* is multiplication. More clearly as in Westhoff (2006), a privacy homomorphic encryption scheme can be denoted as in the following formula:

$$x \; OPERATOR \; y = D_k[E_k(x) \; OPERATOR \; E_k(y)]$$

After the PH had first been investigated by Rivest (1978) and had been mathematically proven that it is prone to ciphertext-only attacks, there have been many researches on its use in different areas. In Domingo-Ferrer (1996) and Domingo-Ferrer (2002) the homomorphic encryption mechanisms based on PH were proposed for the first time. Then, Girao (2004) introduced the concealed data aggregation concept which facilitates data aggregation by homomorphic encryption in WSN. Some alternative

methods for the aggregation of encrypted data in WSN through PH were also proposed by Castelluccia (2005) and Castelluccia (2007). Yet another asymmetric homomorphic encryption technique with a performance analysis for an application-specific scenario for tree based WSN is presented by Viejo (2011). All those publications have focused on the use of PH in WSNs from a particular point of view. When they concentrated on a general application, they could not probably extend the solution to all different topologies; likewise, when they concentrated on general topologies including the tree-based WSN infrastructures they could only propose solution to specific application scenarios.
Nevertheless, the researchers have been trying to offer solutions to the drawbacks in the use of homomorphic encryption in WSN. There are still many open issues to carry on research on this subject; with this motivation the followings may be the research directions: Number theoretical restrictions on the functional operators, such as addition, multiplication, mixed operation; the investigations on the resilient (Wagner, 2004) and precise calculations on data aggregation; homomorphic encryption techniques operating on the real number data instead of only integer data; facilitating the tree based WSN hierarchies instead of only star networks or cluster-based WSN topologies; last but not least, any new proposal of or any extension modification to concealed data aggregation mechanisms based on PH.
As considering the first challenge issue of the energy constrained networks to be the network lifetime and another challenge issue of the wireless networks to be the secure data communication, the academia have been studying the PH use for data aggregation in WSNs over a decade now and it still seems to be an open research issue for academia and the industry as well in the coming years.

Overhearing

Conceptually, overhearing a packet in a wireless network may help a node to monitor the communication around it. Terminology of overhearing may refer to the behavior of either an adversary or a legitimate node. From the perspective of the adversaries, overhearing is a general behavior of passive or active attackers of hearing the wireless communication between the legitimate sensor nodes without their awareness. From the view of the legitimate sensor nodes, overhearing may be used for securing the transmission between the neighbor nodes; in this manner, the nodes themselves can monitor their own packets when routed by their corresponding forwarding nodes. In this section the overhearing issue is discussed for its help on detection of any modification on the forwarding packet where all sensor nodes know that some part of the neighboring nodes knowingly overhear their packets at their forwarding time.
There have been many researches in wireless networks literature that use overhearing concept for the benefit of the total energy consumption of the network. One of them, (Lim, 2005) studied on the appropriate balance in overhearing amounts. Overhearing may be used in favor of underlying routing protocol of the MANETs, however overhearing by any node at any time in an uncontrolled way will probably give a poor communication design regarding to the energy cost. Lim (2005) proposed a randomized communication mechanism by which the set of nodes and the amount of overheard transmissions are to be balanced in MANETs. Lim (2005) compared their scheme against the power saving mechanism and on-demand power management protocol of IEEE 802.11 and showed that their proposal is more energy efficient in terms of both total energy consumption and the energy consumption variance among the nodes.
Brownfield (2006) and Le (2007) also suggested controlling the message overhearing to facilitate the MAC protocol of WSNs for energy savings. Brownfield (2006) proposed in their Gateway MAC (GMAC) protocol to reduce the number of sensor nodes overhearing by controlling the transmission requests and also transition times to sleep state among nodes. GMAC also suggests extra energy prevention by preventing nodes to overhear unrelated control messages and so allowing them to be able to sleep for longer times regarding to their duty cycle. OBMAC (Le, 2007) is another MAC proposal based on overhearing use. Le (2007) suggested overhearing use to reduce the number of redundant transmissions in the sensor network and to prolong the network lifetime, and also showed with simulations that OBMAC outperforms the standard IEEE 802.15.4 MAC protocol regarding to energy consumption. Iima(2009) and Kanzaki(2010) proposed overhearing based data aggregation method for

WSNs using data interpolation. ODAS (Iima, 2009) uses the spatial data interpolation, and the nodes only send their actual data after comparing it to the previous overheard values and unless they decide that there is trivial information in terms of spatial redundancy. ODAST (Kanzaki, 2010) proposes to reduce the total number of transmitted packets using not only the spatial but also the temporal correlation of sensed data based on the previous overheard communication around. However, processing the sensed payload data in the overheard messages might give a delay to the whole system. The investigation of overhearing use in delay-tolerant systems might also be another research subject.

As a common property of the above mentioned studies, overhearing may be used in sensor networks to lead higher energy efficiencies. Any contribution to this subject would be appreciated by the academia and industry since energy efficiency is the first concern of such resource constrained networks. As stated before, the security services have also been the requirements for WSN. Not only for their military based applications but also for the integration of WSNs into any Information System using critical private data, any contribution proposals to the security of the WSN are worth to work on. In this motivation, it is needed to state that overhearing may facilitate the security of the transmitted data to make sure that the forwarded packets are monitored and any modification of the forwarded packets are detected. On the other side, primitive security services such as confidentiality through encryption, authentication and integrity through hash chains may be used in WSNs. Overhearing is not mentioned here as to take place of those services. Nevertheless, overhearing may be seen as another concept to help for reliable communication between the nodes. The scenario is mainly as follows: A node first sends a packet to its parent on the path to the sink node, secondly overhears that packet within the time interval when the parent forwards it to the grandparent. In this scheme, there may also be used encryption or any other service. However, if overheard packet is required to be processed to read the data, it would take much energy consumption on the nodes. There may be used any service that does not require to process the overheard data for their actual meaning. Even, the privacy homomorphic encryption techniques for data aggregation may be used. The forwarding packet may be checked with the previous sent and stored packet in physical bit level without considering the logical meaning of data. The only restriction for theoretical use of overhearing and deciding if the packet is modified is to consciously not change the packet in the protocol. If it's decided that the overheard packet is modified compared to the previous sent packet, a fault will be detected. Detection and recovery mechanisms of such faults are also some other research directions. After a monitoring time period passes, reputation-based trust can be established between the node and its overheard parent according to the observed behavior of the parent. This reputation mechanism may also lead to a framework for the reliable transmission based on overhearing. These are all significant overhearing based issues to research over.

Sensor nodes using the standard IEEE802.15.4 MAC layer protocol consume already a significant amount of their energy for listening. When used, the overhearing presents extra energy consumption for the nodes. To prevent uncontrolled energy consumption due to overhearing at any time and in anywhere, at some times of the communication and/or in some parts of the network the overhearing can be used. Working for optimizing the overhearing use in WSNs may lead to some other valuable solutions. There may also be used probabilistic overhearing mechanisms in which a node occasionally overhears its transmitted packets in terms of a ratio and the parent always behaves as it is monitored in all transmissions since the parent cannot understand overhearing and the ratio is not clearly known by the parent.

Another problematic issue on using overhearing mechanisms in wireless and resource constrained networks is synchronization. Time synchronization problem in WSN has always been a main challenge to solve. Here the issue is not about the general time synchronization in the network, it's partially about the time synchronization between two nodes, child and parent. When the parent forwards the data to grandparent located on the path to the sink, child overhears the same packet. In order to succeed to receive the correct packet at correct time the child requires to know the forwarding time of its parent. Such a system may be established via a scheduling plan. The scheduling plan may statically be given to each node before network deployment. Instead, as generally sensors are deployed without full control mechanisms on their locations, it's better to use a self organizing communication scheduling mechanism

based on the topology of the network. The scheduling plan may be designed in a type of time division approach and the communication may be kept on a TDMA based structure. By this way, at the establishment phase for a self organized WSN, every node can learn its scheduling plan to send, receive, forward and also learn the parent's corresponding forwarding interval to overhear. In contrast, CSMA based infrastructures may also be used dynamically later at any time in any part of the network; whereas the cost of overhearing together with contention would be higher energy consumption. To the authors, these are seen as open research directions about the optimal use of overhearing in WSN.

Integrating IPv6 to WSN

A usual WSN is consisted of massive sensor nodes working for the common objectives in a self organized manner and a sink node as the base station. Such a WSN has a kind of autonomous structure internally. The WSN can be integrated to the external networks (any private or public network of an Information System or the global Internet) through its sink node as being a gateway connection. In some application-specific cases multiple sinks may also be used. The global world uses Internet Protocol as a general routing layer standard, whereas the WSN uses one of various WSN routing protocols based on the application. The general standards for the WSN only define the physical and MAC interfaces for the nodes, but no standard definition is offered for the upper layers. Considering the exchange of the information between the WSN and its integrated IP based network the packet frame formats need to be tuned and a negotiation is required unless the payload of one frame format is fully captured and then recapsulated in the other format. On this motivation, any research on the integration of any different kind of network to WSN and providing their coexistence in ubiquitous environments would be a valuable asset for the pervasive computing.

Indeed, the node devices use IEEE 802.15.4 MAC layer as the standard link layer protocol, which has a specific protocol frame regarding a wireless link throughput of 250 kbps at most (IEEE Std 802.15.4TM-2003). WSN applications consider this and prefer using any convenient routing protocol taking care of not only bandwidth limitation but energy constraint as well. IP packets are not able to be forwarded directly in WSN. It requires a kind of compression on the IP packets to be encapsulated in IEEE 802.15.4 MAC frame. Today the IP packets are considered as both IPv4 and IPv6 structures, the latter is the recent version that expands the IP address notation to 128 bits from 32 bits. The initial deliverables of the standardization process of the Internet Engineering Task Force (IETF) about supporting IPv6 packets over IEEE 802.15.4 networks have been published as RFC 4944 (Montenegro, 2007). The recommendation proposal has been updated in 2011 as RFC 6282 (Hui, 2011) to specify IPv6 header compression format for IPv6 datagrams to be transmitted in IEEE 802.15.4-based networks.

Although the efforts on transmission of IPv6 packets on sensor networks are valuable as the emerging technology is to use IPv6 in the global Internet, there are still open issues for WSN in terms of security considerations. In RFC 4944, it is suggested that the security services provided inherently by IEEE 802.15.4 standard MAC protocol are to be used on the frame data if possible. However, that might not be practical for some applications in terms of the total energy consumption and the network lifetime. It would be an important research to categorize the criteria that require using link layer security service capabilities in 802.15.4-based applications. Another issue stated in RFC 4944 is that the full function devices (FFD) in 802.15.4-based personal area networks may communicate with off-link IPv6 peers and such IPv6 devices may use transmission layer security (TLS) protocol services to secure their communication. TLS mainly aims to provide the security services for an end-to-end secure communication to prevent eavesdropping, tampering, or message forgery. It would not be a big problem for the IPv6 devices to handle a type of TLS mechanism since those devices have no energy limitations. However to handle the similar issues in the sensor devices would lead too much power consumption. In addition to the defense mechanisms to eavesdropping, tampering, or any other attacks defined in Section ATTACKS AND DEFENSE MECHANISMS, those corresponding TLS capabilities may be investigated to be arranged for sensor networks which do not cover a specific transport layer. Taking care of the energy use, similar capabilities could be studied to be handled generally at MAC layer rather than upper

layers. As another approach a way of cross layer design involving MAC and network layers could be studied. Reducing this problem to the issue of securing data frame at MAC layer may also lead the researchers to investigate on the optimal use of security services at link layer in WSN.

Emerging Wireless Sensor and Actor Network Problems

WSNs can be used in many applications where distributed sensing and wireless communicants meet the requirements of the application. Although WSN is a very important technology for today's applications, physical actuation to the environment can be needed by emerging applications where static sensor nodes can be inadequate to handle such operations (Nayak, 2010). Wireless sensor and actor networks (WSAN) are emerging technologies for these types of applications in which actuators are introduced into the sensing area in order to physically effect to the system. The actuators interact with the environment to collect information or to make actions. These actuators can be humans, robots, mobile sensors, etc.

Actuator-based approaches can be new solution perspectives for common problems in sensor networks. For example, one of the fundamental issues is covering all the sensing area by the sensing ranges of the nodes, also known as the sensor coverage problem. Another problem is the connectivity in WSNs in which topology should be a single connected component. Any faults in individual nodes may cause to disrupt connectivity and coverage. In this case, intelligent actuators may move to planned locations or may carry sensor nodes to repair connectivity and coverage. Another fundamental problem, data collection can be solved by mobile actuators. Similar to these approaches, mobile robots may execute other complicated algorithms centrally. For example, security services such as security primitives based on asymmetric cryptography which are not suitable for distributed implementation in resource constraint sensor networks can be implemented on mobile robots centrally.

Although actuator usage brings new solution perspectives to common problems in sensor networks, it causes the formation of new vulnerable points. It could be harder to camouflage mobile actors than doing so the ordinary static sensor nodes. This makes WSAN vulnerable to the actor node tampering. A jamming attack performed by a compromised mobile actor node can be much more harmful than the same attack applied by an ordinary node. The harm will also be much larger for the back-off manipulation, same nonce attack, GTS attack, unintelligent replay attack, replay protection attack, ACK attack, PANId conflict attack, identity spoofing attack and reprogramming attack. Considering this fact, all of these attacks should be reevaluated for WSANs.

CONCLUSION

This chapter mainly investigates the security issues in sensor networks via the following two subjects: an updated attack literature survey and the future research directions on open issues in WSN security.

A detailed survey of the known attacks in WSN is given, the categorization of the attacks according to their target layers are drawn, and the probable defense mechanisms in WSN security literature are also outlined. In addition, some possible suggestions as alternative security approaches are given, such as an available defense mechanism is also proposed to be used as a challenge to defense the sensor network from a GTS attack. The content can be seen as a state-of-the-art reference for the attacks and their defense mechanisms in WSN security.

Although many researches have been made on many issues in WSNs, it is emphasized that there are still many challenges to be faced. Especially considering the pervasive technologies, WSN is a potential environment for any Information System in the future of the ubiquitous platforms. There are many open issues to research on. Our chapter focuses on the future directions for security issues in WSN. To be clear, the significant priorities among the research topics in WSN security are stated with their study motivations. The significance of using trust mechanisms in WSN is underlined. Moreover, any alternative defense mechanism to any attack would be worth to focus on if the energy constraint is taken care of. Among many efforts on WSN security issues some current research directions are indicated. Working on the use of privacy homomorphism and homomorphic encryptions for secure data aggregation in WSN is pointed out, studying the use of synchronized overhearing to secure the communication between nodes is

suggested, the transmission of IPv6 packets on sensor networks is emphasized, and the emerging wireless sensor and actor network problems are listed.
We believe the chapter is a current and timely reference to the attacks and their countermeasures in WSN, and also calls attention to the future research directions in WSN security.

REFERENCES

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A Survey on Sensor Networks. *IEEE Communications Magazine*, *40*(8), 102-114.

Biagioni, E., & Bridges, K. (2002). The Application of Remote Sensor Technology to Assist the Recovery of Rare and Endangered Species. *Special Issue on Distributed Sensor Networks for the International Journal of High Performance Computing Applications, 16*(3).

Brownfield, M.I. (2006). *Energy-Efficient Wireless Sensor Network MAC Protocol.* Doctoral Dissertation (ISBN:0-542-55604-9), Virginia Polytechnic Institute and State University.

Castelluccia, C. (2005). Efficient Aggregation of Encrypted Data in Wireless Sensor Networks. In *MobiQuitous*, (pp. 109-117). IEEE Computer Society.

Castelluccia, C. (2007). Securing Very Dynamic Groups and Data Aggregation in Wireless Sensor Networks. In *Proceedings of the IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems* (pp. 1-9).

Chan, H., & Perrig, A. (2003). Security and Privacy in Sensor Networks. *IEEE Computer, 36*(10), 103-105.

Chang, B. J., Kuo, S. L., Liang, Y. H., & Wang, D. Y. (2008). Markov Chain-Based Trust Model for Analyzing Trust Value in Distributed Multicasting Mobile Ad Hoc Networks. In *Proceedings of the IEEE Asia-Pacific Services Computing Conference* (pp. 156-161).

Deng, J., Han, R., & Mishra, S. (2005). Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks. In *Proceedings of the 1st IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks* (pp.113-124).

Domingo-Ferrer, J. (1996). A New Privacy Homomorphism and Applications. *Information Processing Letters, 60*(5), 277-282.

Domingo-Ferrer, J. (2002). A Provably Secure Additive and Multiplicative Privacy Homomorphism. In *Information Security Conference, Springer LNCS, Vol.2433* (pp. 471-483).

Garcia-Hernandez, C. F., Ibarguangoytia-Gonzalez, P. H., Garcia-Hernandez, J., & Perez-Diaz, J. A. (2007). Wireless Sensor Networks and Applications: A Survey. *International Journal of Computer Science and Network Security, 7*(3), 264-273.

Girao J., Schneider M., & Westhoff D. (2004). CDA: Concealed Data Aggregation in Wireless Sensor Networks. In *ACM Workshop on Wireless Security* (poster presentation).

Hamid, A., Rashid, M. O., & Hong, C. S. (2006). Defense against Lap-top Class Attacker in Wireless Sensor Network. In *Proceedings of the 8th International Conference on Advanced Communication Technology.*

Hoffman, K., Zage, D., & Nita-Rotaru, C. (2009). A Survey of Attack and Defense Techniques for Reputation Systems. *ACM Computing Surveys*, *42*(1).

Hui, J., & Thubert, P. (2011). Compression Format for IPv6 datagrams Over IEEE 802.15.4-Based Networks. *IETF Request for Comments (RFC): 6282*. Retrieved April 20, 2012, from http://tools.ietf.org/html/rfc6282

IEEE Std 802.15.4TM-2003. (2003). IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).

Iima, Y., Kanzaki, A., Hara T., & Nishio, S. (2009). Overhearing-Based Data Transmission Reduction for Periodical Data Gathering in Wireless Sensor Networks. In *Proceedings of the International Workshop on Data Management for Information Explosion in Wireless Networks* (pp. 1048-1053).

Johnson, D. B., & Maltz, D. A. (1996). Dynamic Source Routing in Ad Hoc Wireless Networks. In *Mobile Computing, Kluwer Academic Publishers* (pp. 153-181).

Jung, W., Hong, S., Ha, M., Kim, Y.-J., & Kim, D. (2009). SSL-Based Lightweight Security of IP-Based Wireless Sensor Networks. In *Proceedings of the International Conference on Advanced Information Networking and Applications Workshops* (pp. 1112-1117).

Kanzaki, A., Iima, Y., Hara, T., & Nishio, S. (2010). Overhearing-Based Data Transmission Reduction Using Data Interpolation in Wireless Sensor Networks. In *Proceedings of the Fifth International Conference on Mobile Computing and Ubiquitous Networking*.

Karakehayov, Z. (2005). Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks. In *Proceedings of the Workshop on Real World Wireless Sensor Networks.*

Karlof, C., & Wagner, D. (2002). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. In *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications* (pp. 113-127).

Krontiris, I., Dimitriou, T., & Giannetsos, T. (2007). Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks. In *Proceedings of the 3rd International Conference on Algorithmic Aspects of Wireless Sensor Networks* (pp. 150-161).

Law, Y. W., Hartel, P., den Hartog, J., & Havinga, P. (2005). Link-Layer Jamming Attacks on S-MAC. In *Proceedings of the Second IEEE European Workshop on Wireless Sensor Networks* (pp. 217-225).

Lazos, L., & Poovendran, R. (2004). SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks. In *Proceedings of the 3rd ACM Workshop on Wireless Security* (pp. 21-30).

Le, H-C., Guyennet, H., & Felea, V. (2007). OBMAC: An Overhearing Based MAC Protocol for Wireless Sensor Networks. In *Proceedings of the International Conference on Sensor Technologies and Applications* (pp. 547-553).

Lim, S., Yu, C., & Das, C.R. (2005). Rcast: A Randomized Communication Scheme for Improving Energy Efficiency in MANETs. In *Proceedings of the 25th International Conference on Distributed Computing Systems* (pp. 123-132).

Lopez, J., Roman, R., Agudo, I., & Fernandez-Gago, C. (2010). Trust Management Systems for Wireless Sensor Networks: Best Practices. *Journal of Computer Communications*, *33*(9), 1086-1093.

Lupu, T. G. (2009). Main Types of Attacks in Wireless Sensor Networks. In *Proceedings of the 9th WSEAS international conference on signal, speech and image processing, and the 9th WSEAS International Conference on Signal, Speech and Image Processing, and 9th WSEAS international conference on Multimedia, Internet and Video Technologies* (pp. 180-185).

Mainwaring, A., Culler, D., Polastre, J., Szewczyk, R., & Anderson, J. (2002). Wireless Sensor Networks for Habitat Monitoring. In *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications*.

Misaghi, M., da Silva, E., & Albini, L. C. P. (2012). Distributed Self-Organized Trust Management for Mobile Ad Hoc Networks. *Communications in Computer and Information Science, 293,* 506-518.

Montenegro, G. Kushalnagar, N. Hui, J., & Culler, D. (2007). Transmission of IPv6 Packets over IEEE 802.15.4 Networks. *IETF Request for Comments (RFC): 4944.* Retrieved April 20, 2012, from http://tools.ietf.org/html/rfc4944

Nayak, A., & Stojmenovic, I. (2010). *Wireless Sensor and Actuator Networks: Algorithms and Protocols for Scalable Coordination and Data Communication.* New York, NY: Wiley-Interscience.

Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The Sybil Attack in Sensor Networks: Analysis and Defenses. In *Proceedings of the Third International Symposium on Information Processing in Sensor Networks* (pp. 259-268).

Ns2. Retrieved September 5, 2012, from http://www.isi.edu/nsnam/ns/

OMNeT++. Retrieved September 5, 2012, from http://omnetpp.org/

OPNET. Retrieved September 5, 2012, from http://www.opnet.com/

Padmavathi, G., & Shanmugapriya, D. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. *International Journal of Computer Science and Information Security*, *4*(1&2).

Parno, B. J. (2005). *Distributed Detection of Node Replication Attacks in Sensor Networks*. MSc. Thesis, Carnegie Mellon University.

Pathan, A. S. K. (Ed.). (2010). *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. CRC Press.

Pawar, P. M., Nielsen, R. H., Prasad, N. R., Ohmori, S., & Prasad, R. (2012). Behavioral Modeling of WSN MAC Layer Security Attacks: A Sequential UML Approach. *Journal of Cyber Security and Mobility*, *1*(1), 65-82.

Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., & Culler D.E. (2002). SPINS: Security Protocols for Sensor Networks. *Wireless Networks, 8*(5), 521-534.

Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in Wireless Sensor Networks. *Communications of the ACM, 47*(6), 53-57.

Radosavac, S., Crdenas, A. A., Baras, J. S., & Moustakides, G. V. (2007). Detecting IEEE 802.11 MAC Layer Misbehavior in Ad Hoc Networks: Robust Strategies against Individual and Colluding Attackers. *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks*, *15*(1), 103-128.

Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Computing*, *7*(1), 74-81.

Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On Data Banks and Privacy Homomorphisms. *Foundations on Secure Computation*, Academia Press, 169-179.

Schwiebert, L., Gupta, S. K. S., & Weinmann, J. (2001). Research Challenges in Wireless Networks of Biomedical Sensors. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking* (pp. 151-165). New York: ACM.

Sen, J. (2009). A Survey on Wireless Sensor Network Security. *International Journal of Vommunication Networks and Information Security, 1*(2), 55-78.

Sharma, S., & Jena, S. K. (2011). A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks. In *Proceedings of the International Conference on Communication, Computing & Security* (pp. 146-151).

Singh, V. P., Jain, S., & Singhai, J. (2010). Hello Flood Attack and Its Countermeasures in Wireless Sensor Networks. *International Journal of Computer Science, 7*(3), 23-27.

Sokullu, R., Dagdeviren, O., & Korkmaz, I. (2008). On the IEEE 802.15.4 MAC Layer Attacks: GTS Attack. In *Proceedings of the Second International Conference on Sensor Technologies and Applications* (pp. 673-678).

Sokullu, R., Korkmaz, I., & Dagdeviren, O. (2009). GTS Attack: An IEEE 802.15.4 MAC Layer Attack in Wireless Sensor Networks. *IARIA International Journal On Advances in Networks and Services*, 2(1), 104-114.

Sokullu, R., Korkmaz, I., Dagdeviren, O., Mitseva, A., & Prasad, N. R. (2007). An Investigation on IEEE 802.15.4 MAC Layer Attacks. In *Proceedings of the International Symposium on Wireless Personal Media Communications.*

Srinivasan, A., Teitelbaum, J., Liang, H.,Wu, J., & Cardei, M. (2008). Reputation and Trust-based Systems for Ad Hoc and Sensor Networks. In A. Boukerche (Ed.), *Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks.* Wiley.

Srivastava, M. B., Muntz, R. R., & Potkonjak, M. (2001). Smart Kindergarten: Sensorbased Wireless Networks for Smart Developmental Problem-solving Enviroments. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking* (pp. 132-138). New York: ACM.

Stajano, F., & Anderson, R. (1999). The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In *Proceedings of the 7th International Workshop on Security Protocols.*

Sun, Y., Han, Z., & Liu, K. J. R. (2008). Defense of Trust Management Vulnerabilities in Distributed Networks. *IEEE Communications Magazine*, *46*(2), 112-119.

Viejo, A., Wu, Q., & Domingo-Ferrer, J. (2011). Asymmetric Homomorphisms for Secure Aggregation in Heterogeneous Scenarios, *Information Fusion.* Retrieved April 20, 2012, from http://dx.doi.org/10.1016/j.inffus.2011.03.002

Wagner, D. (2004). Resilient Aggregation in Sensor Networks, In *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*. New York: ACM.

Westhoff, D., Girao, J., & Acharya, M. (2006). Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation. *IEEE Transactions on Mobile Computing, 5*(10), 1417-1431.

Wood, A. D., & Stankovic, J. A. (2004). A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks. *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems.* CRC Press.

Xiao, Y., Sethi, S., Chen, H. H., & Sun, B. (2005). Security Services and Enhancements in the IEEE 802.15.4 Wireless Sensor Networks. In *Proceedings of IEEE GLOBECOM*, *3*.

Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures. *Journal of Network and Computer Applications*, *35*(3), 867-880.

KEY TERMS AND DEFINITIONS

Sensor: A small electro-mechanical device that senses/measures the amount of a relevant physical/environmental data.

Wireless sensor network: A wireless and ad hoc network that is composed of a large number of self-organizing sensor nodes.

Adversary: A malicious node/entity that either attacks to a part of the network or disrupts the operation of legitimate nodes/users in the network.

Guaranteed time slot: A scheduled time slot in IEEE 802.15.4 standard frame format assigned by the coordinator to a device to warrant collision free transmission.

Homomorphic encryption: An encryption technique that performs a mathematical operation on ciphertexts where the result is equal to the output after encrypting the result of the same mathematical operation on the corresponding plaintexts.

Overhearing: Listening the message communication between the other nodes/parties in the neighborhood.

Actuator: A mechanism/entity that interacts with the environment and acts in response to the environment.

Wireless sensor and actor network: A distributed network that involves a large number of sensors and actuators.