Comparative Analysis of Selective Forwarding Attacks over Wireless Sensor Networks

Naser M. Alajmi and Khaled M. Elleithy
Computer Science and Engineering Department,
University of Bridgeport, Bridgeport, CT, USA

ABSTRACT
The potential use of wireless sensor networks (WSNs) in many technological situations is extensive. WSNs are employed in numerous areas, such as battlefields, traffic surveillance, healthcare, and environmental monitoring. Many studies have been conducted to improve various aspects of the performance of WSNs, such as energy efficiency, quality of service (QoS), reliability, mobility, scalability, and extended network lifetime. However, few studies have sought to advance the security of WSNs by focusing on medium access control (MAC), physical, and transport stacks. The network layer is the middle layer that coordinates the lower layers and the upper layers. Thus, the network layer is of paramount significance to the security of WSNs to prevent exploitation of their confidentiality, privacy, availability, integrity, and authenticity. The objective of this study is to address the security laps of WSNs on the network layer, particularly selective forwarding attacks. This paper includes a survey performed from 2003 to 2014. Significant constraints and hazards of physical attacks at the network layer are extensively addressed. The survey includes a benchmark for the comparison of existing approaches for handling the security of WSNs on the network layer and their challenges. Future directions are also comprehensively highlighted in the document. This study will help researchers to understand attacks on the network layer.

Keywords
Wireless sensor network, selective forwarding, and denial of services attacks.

1. INTRODUCTION
Wireless sensor networks contain numerous sensors. These sensors communicate with a vast number of small nodes via radio links. Sensor networks have a source and a base station. The base station controls the sensor networks. They have the ability to collect sensor data and send it to the base station. All data flows between the nodes and the ends at the base station. Nodes are densely deployed [1]. The positions of the nodes do not need to be predetermined. Sensor nodes are deployed in high-risk areas. The majority of WSN protocols do not have the security to prevent simple attacks on the nodes [2]. Thus, sensor network protocol and algorithms should be self-organizing. Some design factors exist for sensor networks and sensor nodes. These factors are significant in the design of protocols or algorithms. The impact of these factors can be used to compare different approaches [3]. The factors include scalability, fault tolerance, network topology, power consumption, production cost, hardware constraints, environment, and transmission media.

The features of sensor nodes guarantee many applications. The rapid deployment, self-organization, and fault tolerance can provide a promising sensing method for certain functions, such as control, communication, and computing [4], [5]. Networks have different applications. Therefore, applications comprise several levels of monitoring, tracking, and controlling. A group of applications is employed for specific purposes. In military applications, sensor nodes include monitoring, battlefield surveillance and object tracking. The battlefield monitors utilized in military operations have prompted the development of WSNs. In medical applications, sensors aid in patient diagnosis and monitoring. The majority of these applications are deployed to monitor an area and react when a sensitive factor is recorded [6].

The security of wireless sensor networks has been extensively investigated over the past few years. WSNs are susceptible to many types of attacks because they serve as an open network with limited resources of nodes. Therefore, the obstacles to securing a wireless sensor network comprise the main disadvantage for all devices. The most conventional threats to the security of wireless sensor networks include eavesdropping, node compromised, interrupt, modify or inject malicious packets, compromised privacy and denial of service attacks [7]. Sensor node can be simply compromised in contrast with wired networks. A common attack in a WSN is a DoS attack; the primary objective of the attacker in a DoS attack is to make WSNs unavailable for users [8]. In a DoS attack, the energy efficient protocols serve as targets in wireless sensor networks. Sensor nodes are liable to physical capture. Because the use of a sensor node as a target is inexpensive, tamper-resistant hardware is unlikely to take over. The denial of a service attack can be affected by draining the energy of sensor nodes to prevent sensor nodes from receiving authentic messages.

Even with physical damage to sensor nodes, which have rendered a network inaccessible, the goal of the attacks is to disrupt the network during the transfer of data [9]. The majority of studies about WSNs can be classified as follows [10]:

Key Management: Establishing and maintaining cryptographic keys in an energy efficient manner to enable encryption and authentication.

Secure Routing: Discovering new protection techniques and applying them to new routing protocols without sacrificing network connectivity, coverage or scalability.

Secure Services: Includes specialized security services such as data aggregation, localization and time synchronization.

Wireless sensor networks are emerging as a central new stage in the information technology ecosystem and an area of active research involving hardware and system design networking, distributed algorithms, programming models, data management, security and social factors [11], [12]. Wireless sensor networks are widely employed in the area that would insure a specific task.

A wireless sensor network is an area of focus by researchers, particularly in the security field. Therefore, one of the main objectives of this survey is the comparison of existing approaches for selective forwarding attacks in WSNs employed by the researchers and developers in the security fields. Sensor nodes have some impacts by selective forwarding attacks. This survey suggests several resolutions for wireless sensor networks in the security field. Section II presents a background of WSNs. Section III describes the denial of a service attack in layers. Section IV compares the selective forwarding attacks between certain approaches. Section V depicts the benchmarks for WSN. Section VI presents the conclusion and recommendations for future studies.

2. BACKGROUND

2.1 Security Goals for WSN

In wireless sensor networks, there are some requirements, which represented the fundamental of security. These requirements should be overall to protect sensitive data, which ensures the operation of the sensor network. The objective of security techniques in wireless sensor networks is to preserve the data from attackers. Attacker motivation and vulnerabilities and opportunities are two factors that give the attacker potential influence over wireless sensor networks [2].

The security goals are categorized as major security goals and minor security goals [13]. Confidentiality, data authentication, data integrity, and data availability are major goals for the security of WSNs. The minor goals include data freshness, access control, and self-organization.

2.1.1 Data Confidentiality

Data confidentiality involves protecting the information hideaway from attackers. The adversaries search for any data in networks; thus, to obscure hidden data hidden from users wishing to modify the data or illegal users, the data should be encrypted with a secret key [14], [15] to ensure protection from eavesdroppers.

2.1.2 Data Authentication

Message authentication is critical in numerous applications in wireless sensor networks. Data authentication is the first prevention that stops any illegal user from participating in the network and original nodes must be distinguishable from unauthorized nodes [14]. Data in this stage should be confirmed for correctness.

2.1.3 Data Integrity

An attempt to modify data is the main issue of adversaries. Therefore, during the transmission data integrity ensures that a received message has not been changed.

2.1.4 Data Availability

If the base station and cluster header fails, the entire sensor network is threatened. A node should be able to locate the resources. Data availability is significant for networks. Therefore, the desired network services should be available even they exist under the denial of a service attack. DoS attacks result in the loss of availability, which may have a detrimental effect [7]. A WSN should introduce these services in every case.

2.1.5 Data Freshness

Data freshness means that the data are not old. It makes sure all data or messages that are not fresh have not been relayed. Therefore, the data must be recent. Although data integrity and confidentiality help to assure data, all messages should attain optimum freshness. The malicious node does not reply to or resend old or previous data [2].

2.1.6 Access Control

Access control restrains the resource that is unauthorized to enter in networks. It has to construct the networks to prevent admittance by unauthorized users.

2.1.7 Self Organization

Sensor nodes must be elastic to be self-organizing and self-healing. The lack of self-organization in a wireless sensor network is risky. Thus, any damage to the output from an attack may be destructive.

Fig 1: WSN Security Requirements

2.2 Constraints for WSN

The limited resources of WSNs include memory, energy, processing power, and transmission channels. Sensor nodes have limited storage and limited communication bandwidth due to the small size of wireless sensor networks. Resource constraints represent the obstacles in wireless sensor networks. Energy and memory are not appropriate for traditional security measures. The condition of resources must assess in WSNs to develop security algorithms.

2.2.1 Limited Memory

Sensor node memory typically includes flash memory and RAM. A sensor is a tiny device with minimal memory and storage space. Thus, a small code size with a few lines should be used for sensor operation and security due to the small size of the memory's storage space [15][62]. In a smart dust project, TinyOS reserve 4500 bytes for security and 4 K bytes for consumer applications [16]. A common sensor type—TelosB—has a 16-bit, 8 MHz RISC CPU with 10 K RAM, 1024 K flash storage and 48 K program memory. Therefore, the algorithms are impractical in sensors [17].

2.2.2 Limited Energy

Sensor nodes use a limited battery. Thus, locating the sensor node in difficult areas such as a battlefield, which has a low battery, is not feasible. Sensors are deployed in dangerous areas in which the battery cannot be modified or exchanged. The energy consumption in sensor nodes can be classified in several parts: communication among sensors, sensor transducers, and microprocessor computation. Power is required for executing 800 to 1000 instructions, in which each bit is transmitted in a WSN [16]. The battery power is limited in sensor nodes. The cost of energy varies. In addition, security levels in WSNs correspond to the energy consumption [18]. In wireless sensor networks, communications and calculations consume the majority of the available energy [6]. Limited energy impacts the process speed and capability of a sensor node.

2.2.3 Unreliable Communication

Sensor nodes use communication to send packets by multi-hop transmission [19]. Unreliable communication hinders the sensor network. A sensor network is susceptible to corruption or damage. Weak packets can cause congested nodes and channel errors [13]. The packets may conflict during a transfer [20].

2.2.4 Higher Latency in Communication

In a wireless sensor network, multi-hop routing and higher latency during transmission may complicate synchronization, which may cause congestion of the network. The security technique is dependent on cryptographic key distribution [21].

3. DENIAL OF SERVICE ATTACKS IN WSN LAYERS

Wireless sensor networks are very weak and susceptible to many types of security attacks on the broadcast. Security attacks are classified into two classes: passive attacks and active attacks [22]. In passive attacks, the attacker compromises data confidentiality. In active attacks, the malicious action targets data confidentiality, data integrity, and unauthorized access. In WSNs, attacks occur in two forms based on the type of hardware utilized by the attacker to compromise the network [2]: mote class attackers and laptop class attackers. Mote class attackers have access to some sensor nodes, such as regular sensor nodes. Malicious nodes are usually gained during node-compromised activities. Laptop class attackers have access to more powerful devices, such as laptops, smart phones, and workstations. The attacks can be classified into two types of attacks: outsider attacks and insider attacks. In an outsider attack, the adversary cannot gain any type of access to the network communications but the network must be pervaded before the attack can be detected. In an insider attack, the adversary gains legitimate and authorized access to the network by neighboring nodes.

A DoS attack is one of the security attacks that impacts wireless sensor networks. It is dependent on the vulnerability of each layer. A DoS attack is a multilayer attack that can launch from any layer in the network. Different types of DoS attacks can impact sensor nodes and can also affect idle nodes or standby mode. A DoS attack comprises the main energy consumption attack in WSNs. Thus, its main focus is network resources. It can also disrupt wireless transmission and can occur either unintentionally in the form of interference, noise or collision at the receiver side or at in the context of an attack [7]. Attackers must reach certain targets, such as network access, network infrastructure, and server applications. The DoS attack attempts to drain the resources available to the victim node by transferring unnecessary data. Therefore, it prevents users from accessing services. This type of attack is intended not only for adversaries who wish to subvert, disrupt, or destroy a network but also for any event that diminishes a network's capability to provide a service [23]. Thus, a DoS attack renders a service unavailable for the users. Several types of attacks to the networks exist, such as consumption of bandwidth or processor time, disruption of service to a system or user, and disruption of physical components.

Karlof [2] noted the names of some types of DoS attacks, such as spoofed data, selective forwarding, the sinkhole attack, the Sybil attack, the wormholes attack, the hello flood attack, and acknowledgment spoofing. Therefore, DoS attacks are severe impacts on most layers of sensor networks. Because a DoS attack comprises a dangerous threat to a wireless sensor network, studies have explored various mechanisms to detect these types of attacks. The important aspect of a DoS attack is the identification of the nodes that are harmed by the adversary.

There are some methods to prevent DoS attacks such as payment for network resources, pushback, strong authentication and identification of traffic [23]. Some mechanism can be implemented to safeguard the reprogramming process, for example, authentication flows. The choice for a DoS attack is the recreate the key request packet, which is came from the sensor node while the lifetime of the keys has expired. If the rate of recreate the key requests is frequently, the sink can conclude the occurrence of a DoS attack and drop the packet from the node for a configurable period of time [24].

Karlof and Wagner [2] have proposed a design for sensor network security and presented different types of threats in ad hoc networks that may reverse the sensor security. Arazi, Qi, and Rose have proposed a RSA based on a framework to prevent DoS attacks and ensure that malicious nodes exhaust the resources [25]. Advancements in wireless sensor networks are being achieved in several fields. Therefore, security in WSNs is an active research field [26].

Denial of services is illustrated for several types of attacks at different layers. At the physical layer, a DoS attack may cause jamming and tampering. At the network layer, it may cause black holes, spoofing, replying, and homing. At the link layer, it may cause collisions and unfairness. At the transport layer, it may cause flooding and de-synchronization [27].

3.1 Physical layer

The physical layer is responsible for the establishment of certain functions, such as connection, modulation, data rate, data encryption, and signal detection. In addition, a physical layer in a network may increase the reliability by reducing the path loss effect and shadowing. Attacks that affect the physical layer include jamming and tampering.

3.1.1 Jamming

Jamming is a type of DoS attack in the physical layer. Because the physical layer is responsible for frequency selection, carrier frequency generation, signal detection, and data encryption and is the lowest layer, it is the first layer to be attacked via jammers [28]. Malicious nodes use the same frequency in the network. Therefore, jamming the entire network will damage the network. An attacker attempts to transfer many packets in different paths to jam the networks. In addition, limited resources lure the adversaries to attack networks.

3.1.2 Tampering

Tampering involves circuitry or injecting fabricated code in a legitimate node. The intruder captures the node by changing its programming code. Thus, attackers may attempt to acquire sensitive information, such as the cryptography key from a node, by destroying it to gain access to a higher level of communication [29]. It affects the physical layer when the sensor nodes are unattended after deployment.

3.2 Data Link Layer

The guarantee interoperability communication between sensor nodes is the main objective of the data link layer. It is responsible for error detection, multiplexing, prevention of collision of packets and transmission. The data link layer impacts security attacks as follows:

3.2.1 Collision

A collision attack executes between two nodes during transmission in a channel. It occurs when the two nodes attempt to transmit using the same frequency. It affects all transmitted packets. The error correction code can be employed to protect the link layer from this type of attack [30].

3.2.2 Medium Access Control (MAC)

MAC layer protocols are designed for wireless sensor networks. A MAC protocol employs different algorithms to conserve battery power [31]. Using low power modes for a radio conserves the battery power when sending or receiving data. The main attack in a MAC protocol is the denial of sleep attacks. The denial of sleep attacks is against the S-MAC protocol [32], which employ a static cycle. Sensor nodes in this protocol are organized into virtual clusters using SYNC messages. Using this protocol, radio networks will be asleep 90% of the time. The T-MAC protocol [33] is superior to the S-MAC protocol by focusing all traffic at the beginning of the period. Because it used the same SYNC technique, the technique enables nodes to transition to sleep mode. B-MAC [34] used a technique that is referred to as low-power listening (LPL). This technique is used to reduce energy consumption. G-MAC [35] is an energy efficient MAC protocol that is designed to coordinate transmissions in clusters.

3.3 Transport Layer

The main objective of the transport layer is to provide reliability and congestion. Many protocols are designed to provide these two tasks. However, they employ different techniques.

3.3.1 Flooding

Flooding attack is a problem that impacts the transport layer. The attacker establishes a connection request until resources are drained. Connection via a puzzle is a potential solution [29].

3.3.2 De-synchronization Attack

De-synchronization is another attack in the transport layer. This attack occurs when there is connection between two endpoints. Therefore, the adversary creates inaccurate messages at the endpoints [29].

3.4 Application Layer

Collection, management and processing of the data are the main functions of the application layer. The objective of the application layer is to render the final output. Therefore, it ensures that the information flows to lower layers. The application layer consists of user data and supports many protocols, such as HTTP, FTP, SMTP, AND TELNET, which provides vulnerability to attacks. The major attack in the application layer is an attack on reliability and data aggregation distortion. The adversary in this attack needs to determine the communication route to alter data using that route. In addition, the adversary creates faulty data via network connections. Therefore, sensor nodes will be harmed by the energy consumption attack when responding to the false data. Ensuring reliability acknowledgment for all received data is the main task of security to prevent attacks on reliability [36].

3.5 Network Layer

The goal of the network layer is to establish a path for efficient routing techniques. Therefore, the main function in the network layer is routing. The network layer is also responsible for some network tasks, such as routing the data between nodes, routing the data from a node to the base station, and routing data between a node and a cluster head. Several challenges at the network layer exist based on applications. These challenges include limited memory, efficiency, reliability, scalability, and energy consumption [37]. The attack of the network layer from several types of attacks impacts these challenges. Routing in the network layer may have caused one of these attacks. Consequently, most network layer attacks against sensor networks may be categorized as one of the following attacks: spoofing or replaying information, selective forwarding, the sinkhole attack, the Sybil attack, and the wormhole attack.

3.5.1 Spoofing or replaying information

This type of attack directly impacts routing information. Creating routing loops, extending or shortening service routes, generating false error messages, and increasing end-to-end latency are caused by the spoofing attack [2].

3.5.2 Selective forwarding

In networks, attackers focus on two types of attacks: a data attack and a routing attack. A selective forwarding attack is a type of data attack, in which a compromised node selectively drops a packet. Thus, a selective forwarding attack may damage the network efficiency. This type of attack can be considered to be a special case of black hole attack. Karlof and Wagner [2] described a selective forwarding attack. They noted that a selective forwarding attack is also known as a malicious node. It is located in the path of data flow that can reject a certain or particular sensitive message that originates from other nodes to forward it to the base station [9]. Subsequently, a malicious node can cut off certain nodes from the base station. A malicious node selectively drops sensitive packets, such as a packet that reports enemy tank movement. Malicious sensor nodes can function as normal sensor nodes [38]. Bysani and Turuk [19] characterize selective forwarding attacks into two classes: drop packets in certain nodes and drop packets of certain types.

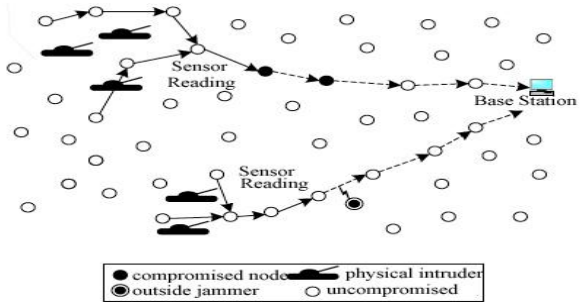

Fig 2: Sensor network under selective forwarding attacks – Redrawn [39]

Military surveillance is very important in battlefields. In the military applications, a sensor node is battery powered and has a constraint of sensing. It also has wireless communication abilities. When need to follow activities, such as tank movements, (Figure 2) sensor readings gather information to create a report. The report will be sent to the base station. Therefore, it can transfer some actions to the objective area. Errors in these actions are possible via a selective forwarding attack. In a selective forwarding attack, malicious nodes serve as standard nodes.

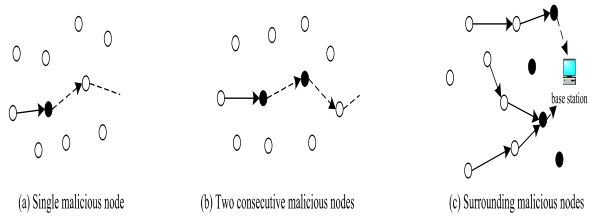

Fig 3: Selective Forwarding based on node – Redrawn [39]

Three fundamental methods apply to any malicious node (Figure 3) [39]. These methods can impact networks. The first method involves a single malicious node. The node, which is located in the middle of the path, can selectively forward packets to the base station. The second method involves two consecutive malicious nodes. In this method, packet dropping is hard to detect because more than one malicious node is forwarded. The last method involves the surrounding malicious nodes, which can reject any packet to the base station.

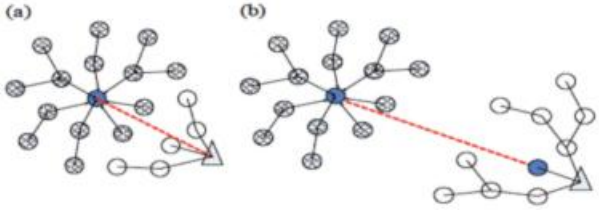

Fig 4: Sinkhole attack in wireless sensor networks. (a) Using an artificial high quality route; (b) Using a wormhole – Redrawn [49]

3.5.3 Sinkhole Attack

One of the DoS attacks types is sinkhole attack. Sinkhole attack is a significant attack. It makes the base station to acquire the whole data and thus create a severe major threat to layer application (Figure 4). Sinkhole attacks comprise one type of network layer attack. In addition, a compromised node sends false routing information to its neighbors to attract network traffic to itself [40]. In a sinkhole attack, the attacker's objective is to tempt the majority of the traffic from a specific location in the network via a compromised node, which generates a metaphorical sinkhole with the attacker at the center [2]. For example, when the node at the coordinator is attacked from an adversary, all other nodes follow it into the sinkhole.

The major chance in a sinkhole attack is eavesdropping. A compromised sensor node attempts to impact the information sent to it from any neighboring node. Therefore, a sensor node eavesdrops on the information is being communicated to its neighboring sensor nodes. Sinkhole attacks ordinarily function by establishing a compromised node that seems attractive to surround the nodes with regard to the routing metric. For instance, the attacker could spoof or reply to an advertisement for a very high quality route to the base station [2]. Karlof and Wagner noted that the sensor nodes are vulnerable to the sinkhole attack based on the communication design. Some security attacks, such as selective forwarding or eavesdropping, can be started during a sinkhole attack. The malicious node or even the attacker can do anything in the network as long as the data are routed through the malicious node. WSNs are vulnerable to sinkhole attacks because many nodes transfer data to a single base station [41]. A sinkhole attack is always searching for nodes located near the base station.

3.5.4 Sybil attack

The Sybil attack is defined as a malicious device that assumes numerous identities [42]. Malicious nodes can allege to have many identities. WSNs are vulnerable to the Sybil attack. In this a case, a node can act as more than one node using different identities of legitimate nodes. Therefore, a single node presents multiple identities to other nodes in the network [43]. The Sybil attack has attempted to degrade the integrity of data, security and resource utilization [11]. James et al. [44] developed a classification for the Sybil attack. They presented direct vs. indirect communication, fabrication vs. stolen identities, and simultaneity as three dimensions. They proposed defenses against the Sybil attack in sensor network, including radio resource testing, verification of key sets for random key pre-distribution, and registration and position verification.

3.5.5 Wormhole attacks

This type of attack is an important and also it is a dangerous attack. The attacker could record a packet at a single location in the network, tunnels them to another location, and resends them into the network [2]. The attacker can replay messages to any part of the network. In wormhole attacks, malicious nodes can create a hidden channel between sensor nodes [45]. A wormhole attack is an important threat to a wireless sensor network because this type of attack does not require that a sensor in the network be compromised. This type of attack affects the network layer by continuously hearing and recording data [46]. It can be implemented in the initial phase when the sensor launches to discover information.

A wormhole attack is not easy to detect because an attacker uses a private band, of which the network is not aware [2]. The technique for detecting a wormhole attack was proposed by Perrig et al. [45]. It is based on packet leashes, and a message includes a timestamp and the location of the sender. However, it requires strict time synchronization and is infeasible for most sensor networks. Wormhole and sinkhole attacks are sometimes combined to attack the sensor networks. These two types of attacks render the networks hard to defend against attacks [2].

3.5.6 HELLO flood attacks

The attackers in HELLO flood attacks send or replay a routing protocol [2]. This protocol consists of HELLO packets, which transmit between sensor nodes with extra energy. HELLO packets are employed as a weapon to encourage the sensors in WSNs. The victim nodes attempt to go through the attacker because they think that the attacker is their neighbor [2]

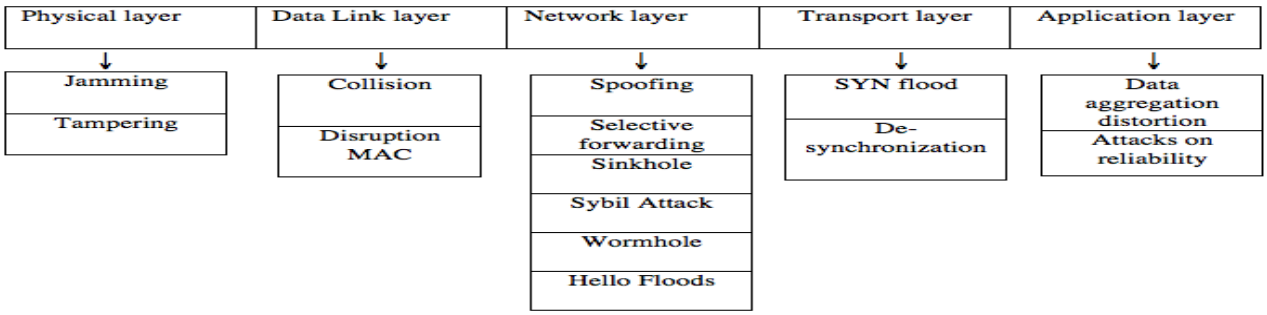

Fig 5: Taxonomy of attack

4. SELECTIVE FORWARDING ATTACKS –DETECTION APPROACHES

In this section, the discussion of countermeasure for selective forwarding attacks is the main goal of this survey. The denial of service attack creates assortments to attack wireless sensor networks. These assortments may temper sensor nodes and the function of networks. Consequently, some attackers target layers, such as the physical layer, the network layer, the link layer, and the transport layer, and some attackers target the routing layer. A DoS attack may occur in any layer of an OSI layer. All DoS attacks are dependent on the vulnerability of each layer in the architecture of wireless sensor networks. In a DoS attack, adversaries attempt to decipher a system but are unsuccessful. The selective forwarding attack is such an attack.

A selective forwarding attack is hard to detect due to unreliable sensor wireless communications. Karlof and Wagner [2] discussed the selective forwarding attack. In this type of attack, malicious nodes have attempted to stop the packets in a network by rejecting message forwarding. According to [2], selective forwarding attacks can impact some multi-hop routing protocols, such as TinyOS beaconing, DSR, PSFQ, directed diffusion and its multipath variant, and geographic routing (GPSR and GEAR). During the launch of a selective forwarding attack, a compromised node has notable prospects, including itself, along the path of data. Based on previous studies, this type of attack makes the sensor network rely on the redundancy forwarding via broadcast for data to spread during the network.

Karlof et al. [2] suggested the prevention of selective forwarding attacks by counting the selective forwarding attacks using multipath routing between nodes, which has disadvantages. Communication overhead is increasing, which causes an increase in the number of paths [39]. In addition, the security of WSNs cannot be resilient. The malicious node forwards several packets to the neighbors but drops some them, which causes a significant loss of data. The Low Energy Adaptive Clustering Hierarchy (LEACH) protocol, which was improved by Wu, Hu, and Ni to the SS-LEACH algorithm, can prevent a selective forwarding attack using a sequence number. Thus, the cluster head is responsible for sending a packet. In addition, the cluster head can discover the attack and send a warning to the base station [47].

Yu and Xiao [39] proposed a new approach based on lightweight security to detect a selective forwarding attack in the environment of sensor networks. The detection utilized a multi-hop acknowledgment to launch alarms by obtaining responses from the nodes that are located in the middle of paths. Yu and Xiao assumed that the approach could identify malicious sensor nodes. The aim of the approach is to send an alarm when a malicious node is discovered, which indicates a selective forwarding attack. The authors noted that the detection accuracy of their approach exceeds 95% with an error rate of 15%.

The detection approach enables the base station and source nodes to aggregate attack alarm information from a specific node. Thus, the specific node that is located in the middle of a route can detect an attack and send an alarm. The detection contains three types of packets during transmission: report, ACK, and alarm. When the node sends a packet, three values are reported: ACK_Cnt, ACK_Span, and ACK_TTL.

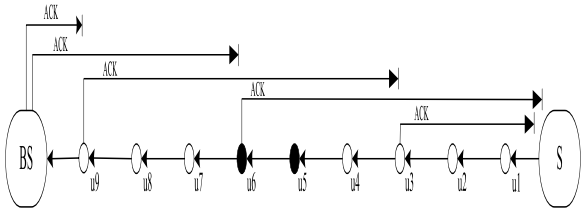

Fig 6: An example of multi-hop acknowledgement with ACK_Span=3, ACK_TTL=6. -Redrawn [39]

Yu and Xiao employed two detection processes in the scheme: a downstream process (the direction on the way to the base station) and an upstream process (the direction on the way to the source node). In the upstream process, a report packet is created and sent to the base station hop by hop when nodes detect a malicious node. ACK_Cnt is set to ACK_Span, which is a predefined metric. The node that is referred to as the intermediate node saves the packet report as soon as it is received in its cache decreases the ACK_Cnt by one or resets ACK_Cnt to its initial value. The packet report may be sent downstream if ACK_Cnt is 0. Simultaneously, an ACK packet is created and the TTL in the ACK packet is set to ACK_TTL, which is a predefined metric. In the remaining detection process, which occurs downstream, packet loss may occur if the intermediate node receives a report packet that should have Packet_ID for a certain source node. In this case, the node creates an alarm packet, in which Lost_Packet_ID_Beg and Lost_Packet_ID_End describe the range of the lost Packet_IDs, and Suspicious_Node_ID is set to the upstream node, where the report with the discontinuous Packet_ID originated. The base station will receive the alarm packet and forward multiple hops that are produced by the node.

The detection accuracy is increased by a detecting selective forwarding attack scheme. Although the radio frequency status is poor, detection accuracy is guaranteed. The scheme authorizes the base station and source nodes to collect attack alarm information from the intermediate nodes. Because the

sensor node requires more effort, it will impact the efficiency of scheme. The scheme cannot develop a countermeasure for other types of attacks; thus, the scalability will be decreased.

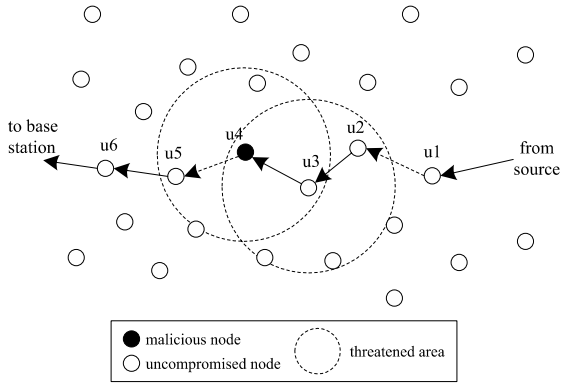

Fig 7: Suspect nodes identification-Redrawn [48]

The identification of suspect nodes is reported via an intermediate node. Figure 7 provides an example of a node that is suspect and detected by an intermediate node. First, Xiao, Yu, and Gao [48] proposed a checkpoint-based method. In this approach, a node is randomly selected as the checkpoint to send an acknowledgement message for detecting the adversary. It is a mechanism used to identify suspect nodes in a selective forwarding attack. They have attempted to improve the technique by detecting an abnormal packet in sensor networks [39]. They assumed that any compromised nodes could not create alert packets with the aim of maliciously prosecuting other nodes. In the previous example, node μ3 produced an alert packet to prosecute node μ4. Thus, the prosecuted node is a compromised node. After collecting evidence to determine whether the node is a malicious node, the source nodes determine the position of the suspect node according to the location. However, it is no guarantee for reliable transmission of messages even though the adversary is positioned by acknowledgement. An acknowledgement packet, an alert packet and a one-way key packet will drain the energy during detection [49].

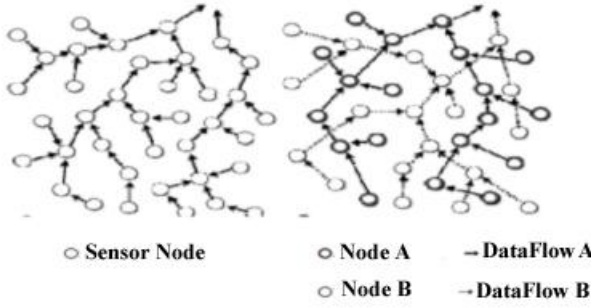

Fig 8: Original sensor nodes after divided into two dataflow topologies-Redrawn [50]

Hung-Min, etal. [50] proposed a multidataflow topology (MDT) scheme against a selective forwarding attack. This scheme divided networks into various data topology, in which a sensor node can communicate with other nodes in the same topology. In figure 6, the sensor nodes are divided into two topologies via the base station. The dataflow topology contains A and B; they encompass the monitored area. One report derives from A or B to control the entire project. The sensing information can be retained via the topology if it does not contain a malicious node; for example, if the attack occurs in topology A, topology B is to transfer the information to the base station because the two topologies are overlapped.

The MDT scheme has some advantages and disadvantages in its defense against a selective forwarding attack. The main advantage of this scheme is that the base station can obtain packets even if the networks are attacked via a selective forwarding attack. Thus, the base station continues to receive information although the node is rendered malicious by an attacker. The disadvantages of a MDT scheme are the high network cost and the low network lifetime. The high cost is attributed to the division of the network into additional data topologies. The network lifetime is low due to multiple data transmissions.

Xin etal, [49] proposed a lightweight defense against a selective forwarding attack. This defense is dependent on the neighboring nodes. Thus, neighboring nodes monitor the packets during packet transmission, assess the attacker's location and retransfer the packets dropped by the attackers. As a result, they suggested that this approach consumes less energy and storage. Its efficiency in detecting selective forwarding attacks ensures packet delivery to the base station. The defense scheme employs a hexagonal WSN mesh topology. According to the hexagonal mesh topology, the authors specified some processes of topology construction, such as node initialization, cell partition, active node election, and secure architecture construction. In node initialization, the node determines its location and its neighbors' locations. In cell partition, the node determines the association with the RC. Active node selection involves contact with nodes of other RCs. The communication relation is determined between RCs to establish and construct a secure architecture.

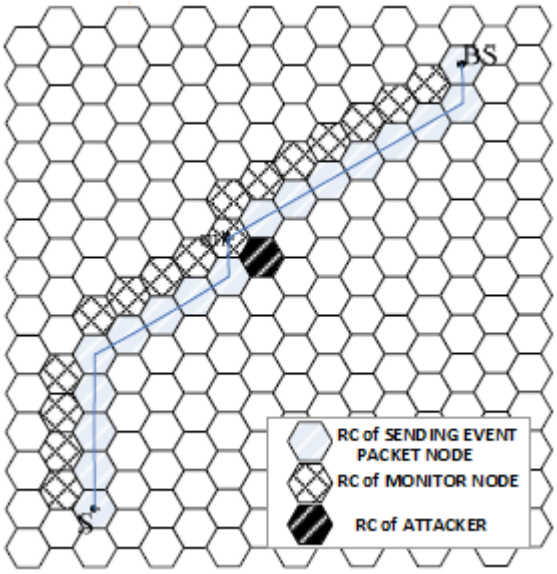

Fig 9: An example for the monitor node gets the attacker-Redrawn [49]

Xin, etal, [49] discussed the two phases of a defense scheme. The first phase is routing discovery and selection. The second phase is data transmission with attack defense. Based on the network model, routing discovery and selection method are designed to prevent selective forwarding attacks. It calculates the number of hops between the source node and the destination node. According to the policy of the probability, it selects the transmission route. A method is employed to randomly create the number of continuous hops. In the

discovery process, they obtain routes with a specific number of hops in each direction via probability schemes. In data transmission, a packet is sent via a source node using a selected process after an event is produced. The source node transfers the event packet to the subsequent hop node. The next hop node, which is referred to as the intermediate node, receives the event packet and neighboring node, which is referred to as the monitor node. The monitor node, which is the neighboring node responsible for detecting the possibility of a selective forwarding attack, resends the event packet to the destination node and sends an alarm message to its neighboring nodes for the location attacker.

The advantages of a lightweight defense scheme are that a share key is not required between nodes because the malicious node is assessed via neighboring nodes. Because one node is active in each RC, the energy will be efficient. The disadvantages are that a GPS is required to achieve the locations of nodes, which increases the cost of the networks. In addition, a change in topology can impact the performance of the defense scheme.

Tran Hoang and Eui-Nam [51] proposed an approach against selective forwarding attacks that consists of a lightweight detection mechanism. The detection is a centralized cluster, which utilized the two-hop neighborhood node information and overhearing technique. It is dependent on the broadcast nature of sensor communication and the high density of sensors. Each sensor node is provided with a detection module that is constructed on an application layer. Sensor node sets routing rules and two-hop neighbor knowledge to generate an alert packet. Hoang and Nam suggested that the two routing rules make the monitoring system more suitable. Thus, the first rule is to determine if the destination node forwards the packet along the path to the sink. It generates an alert packet with the malicious factor α to the sender/source node. The second rule governs that the monitor node waits and detects the packet that was already forwarded along the path to the sink. It verifies the two-hop neighbor knowledge to assess whether the destination node is on the right path to the sink. If not, it generates an alert packet with the malicious factor β to the sender/source node.

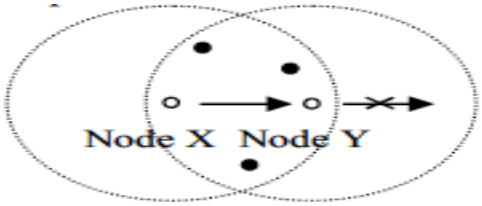

Fig 10: Illustration of monitor node-Redrawn [51]

The detection module is responsible for passively detecting a selective forwarding attack in its neighboring sensor node. The malicious counter is defined as the threshold of abnormal activity in a sensor node, which could not skip. When the malicious counter crossed the threshold X, it revoked the malicious node from its neighbor list. The authors have assumed that the neighboring node should be recognized. The neighboring node must be secure and confidential in the deployment time. The network has a static topology and uses key management to prevent any outside attacks. The selection of one type of network topology prevents the scheme from working with other topologies.

Young Ki Kim etal, [52] proposed the scheme CADE for identifying malicious nodes. This detection scheme does not require time synchronization to detect selective forwarding. It transfers a cumulative acknowledgement to the base station. Thus, authentication occurs between the base station and a node. The detection scheme also provides security against sinkhole attacks. CADE consists three phases: topology construction (the authors suggested the use of SEEM topology construction) and route selection, data transmission, and detection process. The scheme will not work if the topology is changed.

Huijuan Deng etal, [53] proposed a scheme for secure data transmission and detecting a selective forwarding attack. They used watermark technology to detect malicious nodes. Prior to employing a watermark technique, they used a trust value to determine a source path for message forwarding. The trust value involves weighting the credit of each sensor node. The author notes an error rate of 10% and detection accuracy greater than 95%. They assumed that the base station is always trustworthy and cannot be comprised by the adversary, which renders the scheme inappropriate for real wireless sensor networks. Every node has a trust value. At the beginning of network initializing, all nodes should have the same trust value. Huijuan Deng et al. utilized the watermark technique to calculate the packet loss. Data transmission begins when an optimal routing path is confirmed. The base station creates a κ bits binary sequence as the original watermark message. Therefore, a watermark message is part of the packets. A base station compares the extract watermark to the original watermark to detect a selective forwarding attack. The simulation results reveal a channel error rate of 10% and detection accuracy greater than 95%.

Kaplantizs etal, [9] presented a scheme based on support vector machines (SVMs) and sliding windows. The SVM is a class machine-learning algorithm [54]. The scheme is a centralized intrusion detection system. It detects two types of attacks: a selective forwarding attack and a black hole attack. The authors assumed that a sensor node does not spend more energy while adding security features. They used anomaly detection as the basis of IDS and indicated the detection of these attacks with high accuracy without a drain of energy.

Chanatip et al. [55] have proposed a lightweight scheme. They referred to it as a traffic monitor-based selective forwarding attack detection scheme. They used Extra Monitor (EM) to eavesdrop and monitor all traffic when transferring data between nodes. They also employed RSSI to detect a sinkhole attack. The value of RSSI is that four EM nodes can be arranged to establish the positions of all sensor nodes, of which the base station position should be (0,0). Chanatip et al. have assumed that the network is static when sensor nodes are deployed; thus, any change in the type of topology will immediately affect their approach. They assumed that the attackers could capture and damage the nodes. Therefore, all sensor nodes must protect or use tamper robust hardware. These assumptions have caused the detection scheme to drain the energy of the sensor nodes and contribute to the high cost.

5. SECURITY BENCHMARKS

In the last few years, studies of wireless sensor networks have increased. They can be employed in an extensive range of applications, such as weather, military objectives tracking, and patient monitoring. Therefore, these sensor networks need protection from illegitimate users and attackers. Wireless sensor network applications need protection against adversaries who modify, inject, and eavesdrop packets. Some techniques used to prevent DoS attacks include pushback, payment for network resources, robust authentication and traffic identification [23]. Wood and Stankovic suggested that

encryption and authentication techniques could warn network administrators of attacks [29]. Perrig et al. [17] proposed Security Protocols for Sensor Networks (SPINS), which employ two symmetric keys based on security: SNEP and μTESLA. SNEP provides confidentiality, data authentication and data freshness, whereas μTESLA provides an authentication broadcast using a one-way key chain.

Security benchmarks are used to prevent all types of DoS attacks on wireless sensor networks. The following security benchmarks should be included in sensor networks:

5.1 Authentication Protocols

Security is a controversial issue in WSN. Therefore, many protocols serve WSN threats. The Sensor Network Encryption Protocol (SNEP) provides confidentiality of the network. SPINS are designed to provide confidentiality and authentication by combining SNEP and μTESLA; thus, it is an efficient broadcast authentication based on a one-way hash chain [17].

5.2 Encryption

The majority of wireless sensor networks operate in an open area or risky location, which make them susceptible to network attacks. Eavesdropping or adding messages to a network are significant to a WSN [56]. A WSN should adopt key methods of protection, such as message authentication codes, symmetric key encryption and public key cryptography [14]. Law, Dulman, Etalle, and Havinga presented some cryptographic algorithms in sensor networks, in which RC5 and TEA have a capability for the nodes [57].

5.3 Data Partitioning

The technique of partitioning involves the separation of the data in networks into several parts. Deng J. [58] provides a resolve to ensure the attacker cannot take part on data. Data can make it as several packets to ensure that each packet sends to a different route. Hence, the attacker attempts to get all packets from the network, which requires access to the entire network. It is a perfect solution but the energy drain is exorbitant [6].

5.4 Secure Data Aggregation

The transmission of data in wireless sensor network has significantly increased. As a consequence, data traffic is the critical issue in WSNs. The cost of network traffic is very high so to decrease it, wireless sensor nodes collect measurements prior to transferring data to the base station [14]. In wireless sensor network architecture, aggregation is performed in many locations in the network [59].

5.5 Cryptography

Symmetric key cryptography is a key that is employed in cryptography solutions in wireless sensor networks. It is suitable and can be rapidly implemented [6]. Cryptography is used to prevent some security attacks. In wireless sensor networks, applications require protection against injection, eavesdropping, and modification of data; therefore, cryptography is a typical defense.

5.6 Shared Keys

The field of key management focuses on wireless sensor networks. WSN is considered to be a single feature due to size, mobility and power constraints [14]. Four types of keys exist in key management: a global key, a pairwise key node, a pairwise key group, and an individual key. These types of keys give some solution to put the adversary a way from the networks.

Table1: Selective Forwarding Attacks Detection Scheme Analysis

Technique/Features	*Detection Approach*	*Prevention Approach*	*Efficiency*	*Reliability*	*Scalability*	*Energy Consumption*	*Approach Accuracy*	*Approach Nature*	*Routing Protocol*	*Acknowledgement Based*	*Neighbor Monitor*
Karlof and Wagner	X	√	*Moderate*	√	√	*High*	*N/A*	*Distributed*	-	X	X
Yu and Xiao	√	X	*Moderate*	X	X	*High*	*95%*	*Distributed*	*DD, PSFQ*	√	X
Yu and Xiao (CHEMAS)	√	X	*Moderate*	X	X	*High*	*95%*	*Distributed*	*DD, PSFQ*	√	X
Hung-Min Sun et al	X	√	*Low*	X	X	*High*	*N/A*	*Centralized*	-	X	X
Wang Xin-Sheng et al	√	X	*Low*	√	√	*High*	*N/A*	*Distributed*	*OPA_uv wts*	X	√
Tran Hai and Eui Huh (Two-Hops)	√	X	*Moderate*	X	X	*Moderate*	*90%*	*Distributed*	-	X	√
Young Kim et al (CADE)	√	X	*Low*	X	X	*High*	*N/A*	*Centralized*	*SEEM*	√	X
Huijuan Dong et al (Watermark)	√	X	*Moderate*	X	X	*Moderate*	*95%*	*Distributed*	-	X	X
Support Vector Machine (SVM)	√	X	*Low*	√	√	*High*	*80%*	*Centralized*	*MTE*	X	√
Chanatip and Ruttikorn	√	X	*Low*	√	√	*High*	*N/A*	*Centralized*	-	X	√

6. CONCLUSION

Security issues in wireless sensor networks are critical. The significant energy constraints and deployment of sensor nodes in an unattended environment have contributed to the vulnerability of wireless sensor networks. Components that are designed without security can easily become an area for attack. In recent years, the security of WSNs has become increasingly concerning. The use of wireless sensor networks is increasingly employed in environment, commercial, health and military applications. The survey addressed the security laps of WSNs on the network layer, particularly selective forwarding. This paper contains a survey from 2003 to 2014. Significant constraints and hazards of physical attacks are extensively addressed at the network layer. The survey includes a benchmark for the comparison of existing approaches for handling the security of selective forwarding attacks. Its challenges and future directions are comprehensively highlighted in this paper. This survey will help researchers to understand attacks on the network layer. Due to a lack of security, many security attacks to prevent the smooth functioning of wireless sensor networks; examples include denial of sleep and homing. Table 1 summarizes the approaches for the detection of various selective forwarding attacks. Recommendations for future studies include an investigation of the efficiency, scalability, and energy consumption. Some detection approaches require characteristics that may not be appropriate in real scenarios.

7. REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wirelss sensor networks: A survey," Computer Networks, 38(4):393-422, 2002.

[2] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[3] T. Zhu, Z. Zhong, T. He, and Z.-L. Zhang, "Energy-synchronized computing for sustainable sensor networks," *Ad Hoc Networks*, vol. 11, pp. 1392-1404, 2013.

[4] S. H. Lee, S. Lee, H. Song, and H. S. Lee, "Wireless sensor network design for tactical military applications: remote large-scale environments," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, 2009, pp. 1-7.

[5] A. Razaque and K. M. Elleithy, "Energy-Efficient Boarder Node Medium Access Control Protocol for Wireless Sensor Networks," *Sensors*, vol. 14, pp. 5074-5117, 2014.

[6] David Martins, and Herve Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", 2010 IEEE.

[7] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, 47(6):53– 57, June 2004.

[8] Fengyun Li, Guiran Chang and Fuxiang Gao, Lan Yao,"A Novel Cooperation Mechanism to Enforce Security in Wireless Sensor Networks" 2011 Fifth Interantion Conference on Genetic and Evolutionary Computing. IEEE computer society.

[9] Sophia Kaplantzis, Alistair Shilton, Nallasamy Mani, Y. Ahmet S¸ekercio glu,"Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines", Intelligent Sensors, Sensor Networks and Information ,3rd International Conference,pp.335 – 340, IEEE 2007.

[10] K. Loannis and T. Dimitriou, " Toward Intrusion Detection in Wireless Sensor Networks", 13th Euopean Wireless Conference, April 2007, pp. 1-7.

[11] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Sean Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. ICACT 2006, Volume 1, 20-22 Feb, 2006, pp. 1043-1048.

[12] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Val. 47, No. 6, June 2004, pp. 30-33.

[13] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wirelss Sensor Network Security: A survey." Chapter 17, Security in Distributed, Grid, and Pevasive Computing Yang Xiao,(Eds.) pp. Auerbach Publications, CRC Press 2006.

[14] Abhishek Jain, Kamal Kant, and M. R. Tripathy, "Security Solutions for Wireless Sensor Networks", to appear in IEEE ICACCT 2012.

[15] Mayank Saraogi, "Security in Wireless Sensor Networks", University of Tennessee, Knoxville.

[16] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D.E. Culler, K. Pister, "System architectuer directions for networked sensors," in Proceedings of the 9th International Conference on Architictural Support for Programming Languages and Operating System, New York, ACM Press, 2000,pp. 93-104.

[17] A. Perrig, R. Szewczyk, Victorwen, D.E. Culler, J.D. Tygar, "SPINS: Security protocols for sensor networks," Wirelsss Networks, Vol.8, No. 5, pp. 521-534, September 2002.

[18] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, M.B. Srivastava, "On communication security in wirelss adhoc sensor networks," in Proceeding of 11th IEEE International Workshop on Enabling Technologies: Infrastucture for Collaborative Enterprisis (WETICE'02), 2002, pp. 139-144.

[19] L. Bysani and A. Turuk, "A Survey On Selective Forwarding Attack in Wireless Sensor Networks", IEEE 2011.

[20] S. H. Lee, S. Lee, H. Song, and H. S. Lee, "Wireless sensor network design for tactical military applications: remote large-scale environments," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, 2009, pp. 1-7.

[21] J.A. Stankovic et al, "Real-time communication and coordination in embedded sensor networks," Proceeding of the IEEE, Vol. 91, No. 7, pp. 1002-1022, July 2003.

[22] A. Blilat, A. Bouayad, N. Chaoui, and M. Elghazi, "Wireless Sensor Network: Security Challenges", Computer Communication. 2012, IEEE.

[23] David R. Raymond and Scott F. Midkiff,(2008) "Denial-of-Service in Wireless Sensor Networks: Attacks and

Defenses," IEEE Pervasive Computing, val. 7, no. 1, 2008, pp. 74-81.

[24] V. Thiruppathy Kesavan and S. Radhakrishnan, "Secret Key Cryptography Based Security Approach for Wireless Sensor Networks", International Conference on Recent Advances in Computing and Software Systems, 2012 IEEE.

[25] O. Arazi, H. Qi, D. Rose, "A public key Cryptographic Method for DoS mitigation in WSN", IEEE 2007.

[26] Asif Habib, "Sensor Network Security Issues at Network Layer," IEEE 2008.

[27] G. Padmavathi and D. Shanmugapriya,"A survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" International Journal of Computer Science and Information Security, IJCSIS 2009.

[28] Annie Jenniefer and John Raybin Jose,"Techniques for Identifying Denial of Service Attack in Wireless Sensor Network: a Survey" International Journal of Advanced Research in Computer and Communication Engineering , IJARCCE 2014.

[29] A. D. Wood and J. A. Stankovic, "Denial of Service in sensor networks," IEEE Computer, 35(10): 54-62, 2002.

[30] Mohit Saxena,"Security in Wireless Sensor Networks A layer based classifications", Purdue University, West Lafayette, IN 47907.

[31] David R. Raymond and Randy C. Marchany,"Effects of Denial-of-Sleep Attacks on Wireless Sensor Networks MAC Protocols," IEEE Transactions on Vehicular Technology, val. 58, no. 1, 2009.

[32] W. Ye, J. Heidemann, and D. Estrin, "Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks," IEEE/ACM Trans. Netw., val. 12, no. 3, pp. 493-506, Jun. 2004.

[33] T. VanDam and K. Langendoen, "An Addaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks," in Proc. 1st ACM Int. Conf. Embeded Netw. Sensor Syst., Nov. 2003, pp. 171-180.

[34] J. Polastre, J. Hill, and D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks," in Proc. 2nd ACM Int. Conf. Embeded Netw. Sensor Syst., Nov. 2004, pp. 95-107.

[35] M. Brownfield, K. Mehrjoo, A. Fayez, and N. Davis, "Wireless Sensor Networks Energy Adaptive MAC Protocol," in Proc. IEEE Consum. Commun. Netw. Conf., Jan. 2006, pp. 778-782.

[36] P. Mohanty, S. Panigrahi, N. Sarma, and S. Satpathy, "Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey",journal of Theoritical and Applied Information Technology.

[37] A. Razaque and K. M. Elleithy, "Energy-Efficient Boarder Node Medium Access Control Protocol for Wireless Sensor Networks," *Sensors*, vol. 14, pp. 5074-5117, 2014.

[38] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme for power exhausting attacks in wireless sensor networks," in *Ubiquitous and Future Networks (ICUFN), 2011 Third International Conference on*, 2011, pp. 258-263.

[39] Bo Yu and Bin Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks", In Parallel and Distributed Processing Symposiun, 2007. ISSNIP 2006, 20th International, page 8 pp., 2006.

[40] Pandey, A., Tripathi, R.C., "A Survey on Wireless Sensor Networks Security", International Journal Computing Application, IJCA, pp.43-49, 2010.

[41] Nagi, E. C. H., Liu, J. and Lyu, M. R., "Am Efficient Intruder Detection Algorithm Against Sinkhole Attacks in Wireless Sensor Networks", Computer Communication. 6 May, 2007.

[42] M. M. Patel and A. Aggarwal,"Security Attacks in Wireless Sensor Networks: A Survey" International Conference on Intelligent Systems and Signal Processing(ISSP) IEEE 2013.

[43] J. R. Douceur,(2002) "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems(IPTPS"02).

[44] Newsome, J., Shi, E., Song, D, and Perrig, A, "The Sybil attack in sensor networks: analysis & defenses", Proc. of the third international

Symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[45] Yih-Chun Hu, Adrian Perrig, and David B. Johnson,"Packet leashes: A defense against wormhole attacks in wireless sensor networks", IEEE infocom April 2003.

[46] N. Shanti, Lagnesan and K. Ramar, "Study of Different Attack On Multicast Mobile Ad-Hoc Network".

[47] Di Wu, Gang Hu, and Gang Ni,"Research and Improve on Sensor Routing Protocols in Wireless Sensor Networks", IEEE 2008.

[48] Bin Xiao, Bo Yu, and Chuanshan Gao, "CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks", In Parallel and Distributed Processing Symposiun, 2007.

[49] Wang Xin-Sheng, Zhan Yong-Xhao, Xiong Shu-ming and Wang Liang-min, "Lightweight Defense Scheme Against Selective Forwarding Attacks in Wireless Sensor Networks", pages 226-232, IEEE 2009.

[50] Hung-Min Sun, Chien-Min Chen and Ying-Chu Hsiao, "An Efficient Countermeasure to the Selective Forwarding Attack in Wireless Sensor Networks. pages 1-4, IEEE 2007.

[51] Tran Hoang Hai and Eui-Nam Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge" Seventh IEEE Internation Symposium on Network Computing and Applications, 2008, pp.325-331.

[52] Young Ki Kim, Hwaseong Lee, Kwantae Cho, and Dong Hoon Lee, "CADE: Cumulative Acknowledgement based Detection of Selective Forwarding Attacks in Wireless Sensor Networks" Third Internation Conference on Convergence and Hybird Information Technology, 2008, pp.416-422.

[53] Huijuan Deng, Xingming Sun, Baowei Wang, Yuanfu Cao, "Selective Forwarding Attack Detection using Watermark in Wireless Sensor Networks", International Colloquium on Computing, Communications Control, and Management (2009 ISECS), pp. 109-113.

[54] C. Cortes and V. Vapnik, "Support Vector Networks", Machine Learning, vol. 20, no. 3, pp. 273-297, 1995.

[55] Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth, "Detecting Sinkhole Attack and Selective Forwarding Attack in Wireless Sensor Networks", ICICS 2009.

[56] Kalpana Sharma. M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on Mobile Ad-hoc Networks 2010.

[57] Y. W. Law, S. Dulman, S. Etalle, P. Havinga,"Accessing security-critical energy efficient sensor networks" University of Twente, EA Enshede, Netherlands.

[58] Deng J, Han R, and Mishra S. "Countermeasures against Traffic Analysis Attacks in Wireless Sensor Networks", IEEE, 2005, pp. 113-126.

[59] Pathan, A. S. K., Hyung-Woo Lee, and Choong Seon Hong "Security in Wireless Sensor Networks: Issues and Challenges" Advanced Communication Technology (ICACT), 2006.

[60] Yan-Xiao Li, Lian-Qin and Qian-Liang, "Research on Wireless Sensor Network Security", In Proceedings of the International Conference on Computing and Security, 2010 IEEE.

[61] Kalpana Sharma. M K Ghose, Deepak Kumar, Raja Peeyush Kumar Singh, Vikas Kumar Pandey, "A comparative Study of Various Security Approaches Used in Wireless Sensor Networks", In IJAST, Vol 7, April 2010.

[62] V. Kannan and S. Ahmed, "A Resource Perspective To Wireless Sensor Network Security", International Conference on Innovative Mobile and Internet Service in Ubiquitous Computing, IEEE 2011.

8. AUTHOR'S PROFILE

Mr. Naser Alajmi is pursuing towards his Ph.D., Department of Computer Science and Engineering at the University of Bridgeport, Bridgeport, CT. Naser's interests are in Wireless Sensor Network (WSN), Wireless Sensor Network Security, and Network Security.

Dr. Elleithy is the Associate Vice President of Graduate Studies and Research at the University of Bridgeport. He is a professor of Computer Science and Engineering. He has research interests are in the areas of wireless sensor networks, mobile communications, network security, quantum computing, and formal approaches for design and verification. He has published more than three hundred research papers in international journals and conferences in his areas of expertise. Dr. Elleithy has more than 25 years of teaching experience. His teaching evaluations are distinguished in all the universities he joined. He supervised hundreds of senior projects, MS theses and Ph.D. dissertations. He supervised several Ph.D. students. He developed and introduced many new undergraduate/graduate courses. He also developed new teaching / research laboratories in his area of expertise.

Dr. Elleithy is the editor or co-editor for 12 books by Springer. He is a member of technical program committees of many international conferences as recognition of his research qualifications. He served as a guest editor for several International Journals. He was the chairman for the International Conference on Industrial Electronics, Technology & Automation, IETA 2001, 19-21 December 2001, Cairo – Egypt. Also, he is the General Chair of the 2005-2013 International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering virtual conferences.