RESEARCH ARTICLE OPEN ACCESS

Security Attacks and its Countermeasures in Wireless Sensor Networks

Rajkumar, Vani B. A, G. Rajaraman, Dr. H G Chandrakanth
Sambhram Institute of Technology , Bangalore , Karnataka, India

Abstract:
Wireless Sensor Networks have come to the forefront of the scientific community recently. Present WSNs typically communicate directly with a centralized controller or satellite. Going on the other hand, a smart WSN consists of a number of sensors spread across a geographical area; each sensor has wireless communication ability and sufficient intelligence for signal processing and networking of the data. This paper surveyed the different types of attacks, security related issues, and it's Countermeasures with the complete comparison between Layer based Attacks in Wireless Sensor Networks
Keywords: Wireless Sensor Network, Layer based Attacks, Security and Countermeasures.

I. INTRODUCTION

Wireless Sensor Networks have recently emerged as a premier research area. They have great long term economic potential, capability to transform our lives, and create many new system-building challenges. Sensor networks also create a number of new abstract and optimization problems, some of these such as location, exploitation and tracking, are primary issues, in that many applications rely on them for required information. Coverage in general, answers the questions about quality of service that can be provided by a particular sensor network. The combination of multiple types of sensors such as seismic, optical, acoustic, etc. in one network platform and the study of the overall coverage of the system also presents several interesting challenges.

WSN is formed by the collection of sensor nodes, each equipped with its own sensor, processor, radio transceiver and small memory with limited battery power. These nodes are capable of performing some processing, gathering, sensing and communication. Security is a general concern for any network system, but security in WSN is of great importance to ensure its application success [1]. From the security standpoint, it is very essential to provide secure localization, data authentication, data freshness, data confidentiality, data integrity, data availability and time synchronization [2]. Hence the QOS (quality of service) constraints such as memory, computational power, battery power, transmission range should be minimized so that the overhead caused by the security protocols can be light weighted [3].

All these security challenges are encouraging researchers to develop security protocols and algorithms suitable for WSN. A few of the security mechanisms are key management and cryptography, secure time synchronization, secure location discovery, secure routing, trust management system, **s**ecure data aggregation and intrusion detection.

Sensor networks have different constraints than traditional wired networks. Initial, the nodes in sensor networks are probable to be battery powered, and it is frequently very difficult to change the batteries for all of the nodes, as energy conserving forms of communication and computation are essential to wireless sensor networks. Second, since sensors have limited computing power, they may not be capable to run sophisticated network protocols. Third the nodes deployed may be either in a controlled environment where monitoring, maintenance and surveillance are very difficult. Finally in the uncontrolled environments, security for sensor networks becomes extremely difficult.

In this paper we talk about the most common security Attacks and it's Countermeasures in wireless sensor networks and try to give an evaluation of various existing security approaches.

II. Security Requirements in WSNs

A WSN is a special type of network, Shares some commonalities with a typical computer network, but also exhibits many characteristics which are unique to it. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehavior of nodes. The most essential security requirements in WSN are listed below:

***Data confidentiality*:** The security mechanism should ensure that no message in the network is understood by anyone except intended recipient. In a WSN, the issue of confidentiality should address the following requirements [4, 5]: (i) Key distribution mechanism should be extremely robust, (ii) A sensor node should not allow its readings to be accessed by its neighbors unless they are authorized to do so, (iii) Public information such as sensor identity and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks.

***Data integrity*:** The mechanism should guarantee that no message can be changed by an entity as it traverses from the sender to the recipient.

***Availability*:** This requirements ensures that the services of a WSN should be available always even in presence of an internal or external attacks such as a Denial of Service attack (DoS). Different approaches have been proposed by researchers to achieve this goal. While a few mechanisms make use of additional communication among nodes, others advise use of a central access control system to ensure successful delivery of every message to its recipient.

***Data freshness*:** It implies that the data is recent and ensures that no adversary can replay previous messages. This requirement is especially important when the Wireless Sensor Network (WSN) nodes use shared-keys for message communication, where a potential adversary can begin a replay attack using the previous key as the new key is being refreshed and propagated to all the nodes in the Wireless Sensor Network (WSN). A nonce or time-specific counter may be added to each packet to check the freshness of the packet.

Self-organization: Each node in a WSN should be self organizing and self-healing. This feature of a Wireless Sensor Network (WSN) also poses a great challenge to security. The dynamic nature of a Wireless Sensor Network (WSN) makes it sometimes impossible to deploy any preinstalled shared key mechanism among the nodes and the base station [6]. A number of key pre-distribution schemes have been proposed in the context of symmetric encryption [7, 6, 8]. However, for application of public-key cryptographic techniques an efficient mechanism for key distribution is very much essential. It is desirable that the nodes in a Wireless Sensor Network (WSN) self-organize among themselves not only for multi-hop routing but also to carryout key management and developing trust relations.

***Secure localization*:** In many situations, it becomes necessary to accurately and automatically locate each sensor node in a Wireless Sensor Network (WSN). For example, a Wireless Sensor Network (WSN) designed to locate faults would require accurate locations of sensor nodes identifying faults. A potential adversary can easily provide and manipulate false location information by reporting false signal strength, replaying messages. If the location information is not secured properly. The authors in [9] have described a technique called verifiable multilateration (VM). In multilateration, the position of a device is accurately computed from a series of recognized reference points. The authors used authenticated ranging and distance bounding to ensure accurate location of node. Because the use of distance bounding, an attacking node can only enlarge its claimed distance from a recognized reference point. However, to ensure position consistency, the attacker would also have to prove that its distance from another reference point is shorter. As it is not possible for attacker to verify this, it is possible to detect the attacker. In [10], the authors have described a scheme called Secure Range-independent Localization. The scheme is a decentralized range independent localization schemes. It is assumed that the locators are trusted and cannot be compromised by any attacker. A sensor computes its position by listening to the beacon information sent by each locator which includes the locator's position information. The beacon messages are encrypted using a shared global symmetric key that is predistributed in the sensor nodes. Using information from all the beacons that a sensor node receives, it computes its approximate position based on the coordinates of the locators. The sensor node computes an overlapping antenna region using a majority vote scheme. The final position of the sensor node is determined by computing the center of gravity of the overlapping antenna region.

Time synchronization: Most of the applications in sensor networks require time synchronization. Any security mechanism for Wireless Sensor Network (WSN) should also be time-synchronized. A collaborative Wireless Sensor Network (WSN) may require synchronization among a group of sensors. In [11], the authors have proposed a set of secure synchronization protocols for multi-hop sender receiver and group synchronization.

***Authentication*:** It ensures that the communicating node is the one that it claims to be. An adversary can not only change data packets but also can change a packet stream by injecting fabricated packets. It is, therefore, necessary for a receiver to have a mechanism to verify that the received packets have indeed come from the genuine sender node. In case of communication between the two nodes, data authentication can be achieved through a Message Authentication Code (MAC) computed from the

shared secret key among the nodes. A number of authentication schemes for Wireless Sensor Network (WSN)s have been proposed by researchers. Most of these schemes for secure routing and reliable packet.

III. Typical Layer based Attacks in Wireless Sensor Networks

3.1 Attacks in Physical Layer

The physical layer is responsible for carrier frequency generation, frequency selection, modulation, signal detection and data encryption [1]. As with any radio-based medium, the possibility of jamming is there. In addition, nodes in WSNs may be deployed in hostile or insecure environments where an attacker has the physical access. Three types of attacks in physical layer are (i) Jamming (ii) Device tampering and (iii) Eavesdropping

Jamming*:* It is a type of attack which interferes with the radio frequencies that the nodes use in a Wireless Sensor Network (WSN) for communication [12,13]. A jamming source may be powerful enough to disrupt the entire network. Still less powerful jamming sources, an opponent can potentially disrupt communication in the entire network by strategically distributing the jamming sources. Even an intermittent jamming may prove detrimental as the message communication in a Wireless Sensor Network (WSN) may be extremely time-sensitive [12].

Device Tampering: Sensor networks typically operate in outdoor environments. Due to distributed and unattended nature, the nodes in a WSN are highly susceptible to physical attacks [14]. The physical attacks may cause irreversible damage the nodes. The adversary can extract cryptographic keys from the captured node, tamper its circuitry, modify the program codes or even replace it with a malicious sensor [16]. It has been shown that sensor nodes such as MICA2 motes can be compromised in less than one minute time [15].

Eavesdropping*:* Without senders and receivers' awareness, eavesdropping [17, 18, 19] attackers monitor the traffic in transmission on communication channels and collect data that can later be analyzed to extract sensitive information. Wireless Sensor Network (WSN)s are especially vulnerable to such attacks since wireless transmission is the dominant method of communication used by sensors. During transmission, wireless signals are broadcast in the air and thus accessible to the public. Modest equipment, attackers within the sender's transmission range can easily plug themselves into the wireless channel and obtain raw data. By and large, the capability of eavesdropping depends on the power of antennas. The more powerful the antennas, the weaker signals attackers can receive, and the more data can be collected. Since eavesdropping is a passive behavior, such attacks are infrequently detectable.

3.2 Countermeasures in Physical Layer

Some attacks in the physical layer are somewhat hard to cope with. For example, following sensors are deployed in the field, it's difficult to prevent every single sensor from device tampering. Therefore, although there are some mechanisms that attempt to reduce the occurrences of attacks, extra of them focus on protecting information from divulgence.

Access Restriction: Obviously, restricting adversaries from physically accessing or getting close to sensors is effective on all the attacks aforementioned. It is good to have such restrictions if we can, but unfortunately, they are either difficult or infeasible in most cases. Therefore, we usually have to fall back on another type of restrictions: communication media access restriction.

A few techniques exist nowadays that prevent attackers from accessing the wireless medium in use, including sleeping/hibernating and spread spectrum communication [20]. The former is fairly simple as it switches off sensors and keeps them silent until the attackers go away. However, its effectiveness is at the expense of sacrificing the operations of WSNs. The latter is more intelligent, with frequencies varying deliberately. This technique uses either analog schemes where the frequency variation is continuous, or digital schemes (e.g. frequency hopping) where the frequency variation is abrupt. By this way, attackers cannot easily locate the communication channel, and are thus restrained from attacking.

With current technology, powerful devices are required to perform such functionalities. Therefore, spread spectrum communications are not yet feasible for WSNs that are usually constrained in resources. Nonetheless, given the rapid advancement of technologies, this technique is very promising in the future.

Directional antenna [21, 22, 23, 24, 25] is another technique for access restriction. By confining the directions of the signal propagation, it reduces the chances of adversaries accessing the communication channel. Again, similar to spread spectrum communication, its production cost is high at present and unsuitable for large-scale sensor networks, but may be more useful in the long run.

Encryption: In general, cryptography is the all-purpose solution to achieve security goals in WSNs. To protect data confidentiality, cryptography is indispensable. Cryptography can be applied to the data stored on sensors. Once data are encrypted, even if the sensors are captured, it is difficult for the

adversaries to obtain useful information. Of course, the strength of the encryption depends on various factors. A more costly encryption can yield higher strength, but it also drains the limited precious energy faster and needs more memory. More often, cryptography is applied to the data in transmission. There are basically two categories of cryptographic mechanisms: asymmetric and symmetric. In asymmetric mechanisms RSA [26, 27, 28], the keys used for encryption and decryption are different, allowing for easier key distribution. It usually requires a third trusted party called Certificate Authority (CA) to distribute and check certificates so that the identity of the users using a certain key can be verified. However, due to the lack of *a priori* trust relationship and infrastructure support, it is infeasible to have CAs in WSNs. Furthermore, asymmetric cryptography usually consumes more resources such as computation and memory.

3.3 Attacks in Data Link Layer

The link layer is responsible for multiplexing of data-streams, data frame detection, medium access control, and error control [1]. Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation. A collision occurs when two nodes attempt to transmit on the same frequency simultaneously [12]. When packets collide, they are discarded and need to re-transmitted. An adversary may strategically cause collisions in specific packets such as ACK control messages. A possible result of such collisions is the costly exponential back-off. The adversary may simply violate the communication protocol and continuously transmit messages in an attempt to generate collisions. Repeated collisions can also be used by an attacker to cause resource exhaustion [12]. For example, a naïve link layer implementation may continuously attempt to retransmit the corrupted packets. Unless these retransmissions are detected early, the energy levels of the nodes would be exhausted quickly. Unfairness is a weak form of DoS attack [12]. An attacker may cause unfairness by intermittently using the above link layer attacks. In this case, the adversary causes degradation of real-time applications running on other nodes by intermittently disrupting their frame transmissions.

Traffic Manipulation: The wireless communication in WSNs (and other wireless networks) can be easily manipulated in the MAC layer. Attackers can transmit packets right at the moment when legitimate users do so to cause excessive packet collisions. The timing can be readily decided by monitoring the channel and doing some calculations based on the MAC protocol in effect. The artificially increased contention will decrease signal quality and network availability, and will thus dramatically reduce the network throughput [29, 30]. Besides, in widely used MAC schemes where packet transmissions are carefully coordinated, attackers can compete for channel usage aggressively disobeying the coordination rules [31, 32, 33]. This misbehavior can break the operations of the protocols and result in unfair bandwidth usage. In either way, the network performance is degraded. Eventually, the collisions and unfairness lead traffic distortion.

Identity Spoofing: MAC identity spoofing is another common attack in the MAC layer [34]. Due to the broadcast nature of wireless communications, the MAC identity (such as a MAC address or a certificate) of a sensor is open to all the neighbors, including attackers. Without proper protection on it, an attacker can fake an identity and pretend to be a different one. A typical MAC identity spoofing attack is the Sybil attack [35, 36], in which an attacker illegally presents multiple MAC identities.

To gain access to the network or hide, an attacker can spoof as a normal legitimate sensor. It can even spoof as a base station or aggregation point to obtain unauthorized privileges or resources of the WSN. If successful, the entire network could be taken over. Spoofing attacks are usually the basis of further cross-layer attacks that can cause serious consequences.

3.4 Countermeasures in Data Link Layer

To counter attacks in the MAC layer, current research focuses on detection. It allows for many kinds of further actions to stop the attacks, such as excluding the attacking nodes from interactions. There also exist some prevention approaches, which are mainly against spoofing attacks. Many solutions presented below are actually proposed for ad hoc networks. We believe they can be easily extended to wireless sensor networks.

Misbehavior Detection: Because attacks deviate from normal behaviors, it is possible to identify attackers by observing what has happened. Various data can be collected for this purpose, and various actions can be taken after detection.

In a countering scheme [37] for the IEEE 802.11 protocol, a receiver assigns and adjusts the back off values to be used by the corresponding sender. Whenever detecting the sender's misbehavior in manipulating back off value, the receiver may add some penalty to the next back off value assigned to the sender. The idea was applied to ad hoc networks [33], and similarly can also be applied to WSNs.

Identity Protection **:** Identity can be treated as yet another kind of information whose legitimacy needs to be guaranteed. Therefore, cryptography-based

authentication can be used to prevent identity spoofing. Since most authentication schemes are designed for the network layer and the application layer.

Identity-key association [36] can also help to reduce false identities. The key idea is to associate the node identity with keys used by the node in communication. An attacker can impersonate a node in front of another only if the communication key shared by them is cracked.

3.5 Attacks in the Network Layer

The network layer of WSNs is vulnerable to the different types of attacks such as: (i) spoofed routing information , (ii) selective packet forwarding, (iii) sinkhole, (iv) Sybil, (v) wormhole, (vi) hello flood, (vii) acknowledgment spoofing, (viii) *Black Hole,(x) False Routing,(xi) Packet Replication* etc. These attacks are described briefly in the following:

Spoofed routing information: The most direct attack against a routing protocol is to target the routing information in the network. An attacker may spoof, alter, or replay routing information to disrupt traffic in the network [38]. These disruptions include creation of routing loops, attracting or repelling network traffic from selected nodes, extending or shortening source routes, generating fake error messages, causing network partitioning, and increasing end-to-end latency.

Selective forwarding**:** In a multi-hop network like a WSN, for message communication all the nodes need to forward messages accurately. An attacker may compromise a node in such a way that it selectively forwards some messages and drops others [38].

Sinkhole**:** In a sinkhole attack, an attacker makes a compromised node look more attractive to its neighbors by forging the routing information [39, 38, 40]. The result is that the neighbor nodes choose the compromised node as the next-hop node to route their data through. This type of attack makes selective forwarding very simple as all traffic from a large area in the network would flow through the compromised node.

Sybil attack: It is an attack where one node presents more than one identity in a network. It was originally described as an attack intended to defeat the objective of redundancy mechanisms in distributed data storage systems in peer-to peer networks [41]. Newsome et al describe this attack from the perspective of a WSN [39]. In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation, and foiling misbehavior detection. Regardless of the target (voting, routing, aggregation), the Sybil algorithm functions similarly. All of the techniques involve utilizing multiple identities. For instance, in a sensor network voting scheme, the Sybil attack might utilize multiple identities to generate additional "votes". Similarly, to attack the routing protocol, the Sybil attack would rely on a malicious node taking on the identity of multiple nodes, and thus routing multiple paths through a single malicious node.

Wormhole**:** A wormhole is low latency link between two portions of a network over which an attacker replays network messages [38]. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The latter case is closely related to sinkhole attack as an attacking node near the base station can provide a one-hop link to that base station via the other attacking node in a distant part of the network.

Hello flood**:** Most of the protocols that use Hello packets make the naïve assumption that receiving such a packet implies that the sender is within the radio range of the receiver. An attacker may use a high-powered transmitter to fool a large number of nodes and make them believe that they are within its neighborhood [38]. Subsequently, the attacker node falsely broadcasts a shorter route to the base station, and all the nodes which received the Hello packets, attempt to transmit to the attacker node. However, these nodes are out of the radio range of the attacker.

Acknowledgment spoofing**:** Some routing algorithms for WSNs require transmission of acknowledgment packets. An attacking node may overhear packet transmissions from its neighboring nodes and spoof the acknowledgments thereby providing false information to the nodes [38]. In this way, the attacker is able to disseminate wrong information about the status of the nodes.

Black Hole: The black hole attack is one of the simplest routing attacks in WSNs. In a black hole attack, the attacker swallows (i.e. receives but does not forward) all the messages he receives, just as a black hole absorbing everything passing by. By refusing to forward any message he receives, the attacker will affect all the traffic flowing through it. Hence, the throughput of a subset of nodes, especially the neighboring nodes around the attacker and with traffic through it, is dramatically decreased. Different locations of the attacker induce different influences on the network. If the attacker is located close to the base station, all the traffic going to the base station might need to go through the attacker. Obviously, black hole attacks in this case can break the

communication between the base station and the rest of the WSN, and effectively prevent the WSN from serving its purposes. In contrast, if a black hole attacking node is at the edge of the WSN, probably very few sensors need it to communicate with others. Therefore, the harm can be very limited.

False Routing: As the name suggests, false routing attacks [42] are launched by enforcing false routing information. There are three different approaches of enforcement [42]:

• Overflowing routing tables
• Poisoning routing tables
• Poisoning routing caches

Packet Replication: In this type of attacks, attackers resend (replicate) packets previously received from other nodes. The packets can be broadcasted to the entire network (called *flooding attack*), or to a particular set of nodes. They can also resent irrespective of whether the sender is sending any new packets or not. With large amount of packets replayed, both the bandwidth of the network and the power of the nodes are consumed in vain, which leads to early termination of network operations.

3.6 Countermeasures in Network Layer

Since the functionalities of the network layer require the close collaboration of many nodes, all these nodes have to be enclosed for security consideration. It is therefore relatively difficult to mitigate attacks. Nonetheless, some countermeasures are available as follows:
• Routing Access Restriction
• False Routing Information Detection
• Wormhole Detection

Routing Access Restriction: Routing may be one of the most attractive attack targets in WSNs, as we saw in the previous subsection. If we can exclude attackers from participating in the routing process, i.e. restrict them from accessing routing, a large number of attacks in the network layer will be prevented or alleviated. Multi-path routing is one of the methods to reduce the effectiveness of attacks launched by attackers on routing paths [43, 44, 45]. In these schemes, packets are routed through multiple paths. Even if the attacker on one of the paths breaks down the path, the routing is not necessarily broken as other paths still exist. This alleviates the impact of routing attacks, although does not prevent these attacks.

False Routing Information Detection: Sometimes attackers do have chances to send false routing information into the network, e.g. during route discovery stages. If the false information does not lead to network failure such as broken routes, we really cannot do much about it. Otherwise, we can apply the idea of misbehavior detection. For example, watchdog [47] or IDS [51, 48, 49] may find that some node fails to route messages along the routing path due to the wrong information it keeps. This anomaly of route failure may trigger out an alarm. Nodes can start to trace the source of false routing information. Reputation [51, 50] can also be maintained, depending on whether nodes are providing valid routing information. Nonetheless, how to trace the source of routing information can be a very difficult problem.

Wormhole Detection : Wormhole attacks are difficult to deal with because the information they inject into the networks is real. The most recent research work on the countermeasures focuses on the following techniques:

• Using synchronized clocks [46]. With the assumption that all nodes are tightly synchronized, each packet includes the time at which it is sent out. When receiving the packet, the receiver compares this value to the time at which it receives the packet. With the knowledge of transmission distance and consumed time, the receiver is able to detect if the packet has traveled too far. If the transmission distance is far beyond the maximum allowed travel distance, probably it is under wormhole attacks.
• Using directional antennas [21]. Directional antenna is used to discover neighboring nodes identified by zone. The zones around each sensor are numbered 1 to N oriented clockwise starting with zone 1 facing east. After receiving signals from unknown nodes, a node can get approximate direction information based on received signals and identify the unknown node by zone. After that it cooperates with its neighboring nodes to verify the legitimacy of the unknown node, e.g. by checking whether the unknown node is known by the neighboring nodes.
• Using Multidimensional Scaling - Visualization of Wormhole (MDS-VOW)[52]. MDS-VOW first constructs the layout of the network. If there exist wormhole attackers, the shape of the constructed network layout will show some bent/distorted features.

3.7 Attacks in Transport layer

The attacks that can be launched on the transport layer in a WSN are flooding attack and de-synchronization attack.

Flooding**:** Whenever a protocol is required to maintain state at either end of a connection, it becomes vulnerable to memory exhaustion through flooding [12]. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum

limit. In either case, further legitimate requests will be ignored.

***De-synchronization*:** De-synchronization refers to the disruption of an existing connection [12]. An attacker may, for example, repeatedly spoof messages to an end host causing the host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data causing them instead to waste energy attempting to recover from errors which never really exist.

3.8 Countermeasures in Transport Layer

One way to provide message confidentiality in transport layer is point-to-point or end-to end communication through data encryption. Though TCP is the main connection oriented reliable protocol in Internet, it does not fit well in MANET. TCP feedback (TCP-F) [53], TCP explicit failure notification (TCP-ELFN) [53], ad-hoc transmission control protocol (ATCP) [53], and ad hoc transport protocol (ATP) have been developed but none of them covers security issues involved in MANET. Secure Socket Layer (SSL) [54], Transport Layer Security (TLS) [54] and Private Communications Transport (PCT) [54] protocols were designed on the basis of public key cryptography to provide secure communications. TLS/SSL provides protection against masquerade attacks, man-in-middle attacks, rollback attacks, and replay attacks.

3.9Attacks in the Application Layer

Attacks in this layer have the knowledge of data semantics, and thus can manipulate the data to change the semantics. As the result, false data are presented to applications and lead to abnormal actions. In this section, the following attacks will be discussed:

- Malicious Code Attacks
- Repudiation Attacks
- Clock Skewing
- Selective Message Forwarding
- Data Aggregation Distortion

Malicious Code Attacks: Various malicious codes such as virus, worm, spy-wares and Trojan horse attack both operating systems and user applications that cause the computer system and network to slow down or even damaged. An attacker can produce this type of attacks in MANET and can seek their desire information [55].

Repudiation Attacks: The solution that taken to solve authentication or non-repudiation attacks in network layer or in transport layer is not enough. Because, repudiation refers to a denial of participation in the communication. Example of repudiation attack on a commercial system: a selfish person could deny conducting an operation on a credit card purchase or deny any on-line transaction [55].

Clock Skewing: The targets of this attack are those sensors in need of synchronized operations [13, 56, 57]. By disseminating false timing information, the attacks aim to desynchronize the sensors (i.e. skew their clocks).

Selective Message Forwarding: For this attack, the adversary has to be on the path between the source and the destination, and is thus responsible for forwarding packet for the source. The attack can be launched by forwarding some or partial messages selectively but not others. Note that the attack is different from the other selective forwarding attack in the network layer. To launch the selective forwarding attack in the application layer, attackers need to understand the semantics of the payload of the application layer packets (i.e. treat each packet as a meaningful *message* instead of a monolithic unit), and select the packets to be forwarded based on the semantics.

Data Aggregation Distortion: Once data is collected, sensors usually send it back to base stations for processing. Attackers may maliciously modify the data to be aggregated, and make the final aggregation results computed by the base stations distorted. Consequently, the base stations will have an incorrect view of the environment monitored by the sensors, and may take inappropriate actions. Data aggregation can be totally disrupted if black hole or sinkhole attacks are launched. In this scenario, no data can reach the base stations. However, for those attacks, only the network layer knowledge is required. Therefore, they are categorized as network layer attacks.

3.10 Countermeasures in the Application Layer

As presented above, attacks in the application layer rely on application data semantics. Therefore, the countermeasures focus on protecting the integrity and confidentiality of data, no matter it is for control or not.

Data Integrity Protection: In general, authentication can be used to protect any data integrity. Nodes can use end-to-end, hop-to-hop or multipath authentication depending on the cost they can afford and the security level they desire. When authentication is not adopted, e.g. for feasibility reasons, or when data integrity is somehow compromised, the misbehavior detection techniques can be applied. The differences lie in the data to be observed in order to collect proofs of anomalies. Taking the clock skewing attack as an example: to

detect such attacks, timing information in synchronization packets should be watched. When readings (the data collected by sensors about the monitored environment) are considered, some specific detection mechanisms have been proposed, and are referred to as *false reading detection*. With an assumption that the faulty/compromised sensors produce readings remarkably deviated from the normal condition, an outlier detection algorithm [58] can locate such sensors by comparing their readings with those of their neighbors. In the online deviation detection scheme [59], an estimation of the data distribution is computed through the input data stream of the WSN. If the current reading of a sensor remarkably deviates from the data distribution (namely the normal readings in the WSN), this sensor will be detected as an outlier. There is also a centralized approach [60]. Base stations launch marked
packets to probe certain sensors and try to route packets through them. If a sensor fails to respond, the base stations may conclude that this node is dead.

Data Confidentiality Protection: Encryption is an effective approach to prevent attackers from understanding captured data. Similar to authentication, the principles of encryption do not change for use in different layers.

IV. CONCLUSION

Security in wireless sensor networks has attracted a lot of attention in the recent years. In this paper, a survey is given on existing and possible attacks in wireless sensor networks. The attacks are classified according to the OSI stack model. For each layer of Physical, Data link, Network Transport and Application, we have discussed several typical attacks that exploit the characteristics of that layer. We have also covered the countermeasures and potential solutions against those attacks, with the complete comparison between Layer based Attacks in Wireless Sensor Networks and mentioned some open research issues. By reading the paper, the readers can have a better view of attacks and countermeasures in wireless sensor networks, and find their way to start secure designs for these networks.

The evaluation of different Layer based Attacks and possible counter measure in Wireless Sensor Networks have been shown in the table 1.

Table.1. Typical Layer based Attacks and possible counter measure in Wireless Sensor Networks.

S.No.	Layer	Attacks	Counter measure
1	Physical Layer	•Jamming •Node Tampering •Eavesdropping	•.Access Restriction, •Encryption
2.	Data Link Layer	•Traffic Manipulation •Identity Spoofing	•Misbehavior Detection, •Identity Protection
3.	Network Layer	•Spoofed routing information •Sybil attack •Wormhole •Hello flood •Acknowledgment spoofing •Black Hole •False Routing • Packet Replication	•Routing Access Restriction •False Routing Information Detection • Wormhole Detection
4.	Transport Layer	•Flooding •De-synchronization	•Limiting Connection Numbers •Authentication
5.	Application Layer	• Malicious Code Attacks • Repudiation Attacks • Clock Skewing • Selective Message Forwarding • Data Aggregation Distortion	•Data Integrity Protection, •Data Confidentiality Protection

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, August 2002.

[2]. Daojing He,Lin cui,Hejiao Hang,"Design and verification of Enhanced secure localization scheme in wireless sensor network "IEEE Transaction On parallel and distributed systems vol. 20 no.7 July 2009

[3]. S. Uluagac, C. Lee, R. Beyah, and J. Copeland, "Designing Secure Protocols for Wireless Sensor Networks," Wireless Algorithms, Systems, and Applications, vol. 5258, pp. 503-514, Springer, 2008

[4] D.W. Carman, P.S. Krus, and B.J. Matt, "Constraints and approaches for distributed sensor network security", Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, 2000.

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

[6] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks", In *Proceedings of the 9th ACM Conference on Computer and Networking*, pp. 41- 47, Nov 2002.

[7] H. Chan, A. Perrig, and D. Song, "Random key pre-distribution schemes for sensor networks", In *Proceedings of the IEEE Symposium on Security and Privacy*, pp.197, IEEE Computer Society, May 2003.

[8] D. Liu, P. Ning, and R. Li, "Establishing pair-wise keys in distributed sensor networks", *ACM Transactions on Information Systems Security*, Vol. 8, No. 1, pp. 41-77, 2005.

[9] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks", *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, pp. 221-232, 2006.

[10] L. Lazos and R. Poovendran, "SERLOC: Robust localization for wireless sensor networks", *ACM Transactions on Sensor Networks*, Vol. 1, No. 1, pp.73-100, 2005.

[11] S. Ganeriwal, S. Capkun, C.-C. Han, and M.B. Srivastava, "Secure time synchronization service for sensor networks", In *Proceedings of the 4th ACM Workshop on Wireless Security*, pp. 97-106, New York, NY, USA, 2005, ACM Press.

[12] A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", *IEEE Computer*, Vol. 35, No. 10, pp. 54-62, 2002.

[13] E. Shi and A. Perrig, "Designing secure sensor networks", *Wireless Communication Magazine*, Vol. 11, No. 6, pp. 38-43, December 2004.

[14] X. Wang, W. Gu, K. Schosek, S. Chellappan, and D. Xuan, "Sensor network configuration under physical attacks,", Technical report (OSU-CISRC-7/04-TR45), Department of Computer Science and Engineering, Ohio State University, July 2004.

[15] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: The need for secure systems", Technical Report CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.

[16] X. Wang, W. Gu, S. Chellappan, Dong Xuan, and Ten H. Laii, "Search-based physical attacks in sensor networks: Modeling and defense, Technical report, Department of Computer Science and Engineering, Ohio State University, February 2005.

[17] M. Franklin, Z. Galil, andM. Yung, "Eavesdropping games: a graph-theoretic approach to privacy in distributed systems," *J. ACM*, vol. 47, no. 2, pp. 225– 243, 2000.

[18] M. Abadi and J. Jürjens, "Formal eavesdropping and its computational interpretation," in *TACS '01: Proceedings of the 4th International Symposium on Theoretical Aspects of Computer Software*. London, UK: Springer-Verlag, 2001, pp. 82–94.

[19] K. D. Murray, *Security Scrapbook Espionage* and *Privacy News of the Week*. [Online]. Available: http: //www.spybusters.com/SS0210.html.

[20] [Online]. Available: http: //www.faqs.org/rfcs/rfc1455.html

[21] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Network and Distributed System Security Symposium (NDSS)*, 2004.

[22] R. R. Choudhury, X. Yang, N. H. Vaidya, and R. Ramanathan, "Using directional antennas for medium access control in ad hoc networks," in *MobiCom '02: Proceedings of the 8th annual international conference on Mobile computing and networking*. New York, NY, USA: ACMPress, 2002, pp. 59–70.

[23] S. Yi, Y. Pei, and S. Kalyanaraman, "On the capacity improvement of ad hoc wireless

networks using directional antennas," in *MobiHoc '03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*. New York, NY, USA: ACM Press, 2003, pp. 108–116.

[24] M. Takai, J. Martin, R. Bagrodia, and A. Ren, "Directional virtual carrier sensing for directional antennas in mobile ad hoc networks," in *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. New York, NY, USA: ACM Press, 2002, pp.183–193.

[25] R. Ramanathan, "On the performance of ad hoc networks with beamforming antennas," in *MobiHoc '01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*. New York, NY, USA: ACM Press, 2001, pp. 95–105.

[26] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.

[27] J.-P. Hubaux, L. Buttyán, and S. Capkun, "The quest for security in mobile ad hoc networks," in *MobiHoc '01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*. ACM Press, 2001, pp. 146–155.

[28] "Providing robust and ubiquitous security support for mobile ad hoc networks," in *ICNP '01: Proceedings of the Ninth International Conference on Network Protocols (ICNP'01)*. IEEE Computer Society, 2001, p. 251.

[29] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of service attacks at the mac layer in wireless ad hoc networks." [Online]. Available: http://www.cs.ucr.edu/krish/milcomvik.pdf

[30] I. A. Jean-Pierre, "Denial of service resilience in ad hoc networks." [Online]. Available: http://lcawww.epfl.ch/Publications/aad/aadHK04.pdf

[31] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks,"*Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[32] P. Michiardi and R. Molva, "Prevention of denial of service attacks and selfishness in mobile ad hoc networks," in *Institut Eurecom Research Report RR-02-063*, 2002.

[33] A. A. Cardenas, S. Radosavac, and J. S. Baras, "Detection and prevention of mac layer misbehavior in ad hoc networks," in *Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks*, 2004.

[34] E. D. Cardenas, "Mac spoofing–an introduction," 2003. [Online]. Available: http : //www.giac.org/practical/GSEC/EdgarCardenasGSEC.pdf

[35] J. R. Douceur, "The sybil attack," in *IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems*. Springer-Verlag, 2002, pp. 251–260.

[36] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *IPSN'04: Proceedings of the third international symposium on Information processing in sensor networks*. ACM Press, 2004, pp. 259–268.

[37] P. Kyasanur and N. H. Vaidya, "Detection and handling of mac layer misbehavior in wireless networks." in *DSN*, 2003, pp. 173–182.

[38] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications,* May 2003, pp. 113-127.

[39] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses", In *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, pp. 259-268, ACM Press 2004.

[40] A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", *IEEE Computer*, Vol. 35, No. 10, pp. 54-62, 2002.

[41] J. Douceur, "The Sybil attack", In *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02),* February 2002.

[42] C. R. Murthy and B.S.Manoj, "Transport layer and security protocols for ad hoc wireless networks," in *Ad Hoc Wireless Networks - Architectures and Protocols*, 2004.

[43] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 5, no. 4, pp. 11–25, 2001.

[44] W. Lou, W. Liu, and Y. Fang, "Spread: Enhancing data confidentiality in mobile ad hoc networks," in *IEEE INFOCOM*, 2004.

[45] P. Papadimitratos and Z. J. Haas, "Secure data transmission in mobile ad hoc networks," in *WiSe '03: Proceedings of the 2003 ACM workshop on Wireless security*.

New York, NY, USA: ACM Press, 2003, pp. 41–50.

[46] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," 2001. [Online]. Available: citeseer.ist.psu.edu/hu01packet.html.

[47] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*. ACMPress, 2000, pp. 255–265.

[48] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion detection techniques for mobile wireless networks," *Wirel. Netw.*, vol. 9, no. 5, pp. 545–556, 2003.

[49] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*. New York, NY, USA: ACMPress, 2000, pp. 275–283.

[50] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2002, pp. 107–121.

[51] F. K. Andreas, "Sensors for detection of misbehaving nodes in manets." [Online]. Available: http://medien.informatik.uniulm.de/forschung/ publikationen / dimva2004.pdf

[52] W.Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in *WiSe '04: Proceedings of the 2004 ACM workshop on Wireless security*. ACM Press, 2004, pp. 51–60.

[53] H. Hsieh and R. Sivakumar, "*Transport OverWireless Networks,"* Handbook of Wireless Networks and Mobile Computing, Edited by Ivan Stojmenovic. John Wiley and Sons, Inc., 2002.

[54] C. Kaufman, R. Perlman, and M. Speciner, "*Network Security Private Communication in a Public World,"* Prentice Hall PTR, A division of Pearson Education, Inc., 2002.

[55] B. Wu, J. Chen, J. Wu, M. Cardei, "*A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,"* Department of Computer Science and Engineering, Florida Atlantic University, http:// student.fau.edu/ jchen8/ web /papers/ SurveyBookchapter.pdf

[56] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: security protocols for sensor networks," *Wirel. Netw.*, vol. 8, no. 5, pp. 521–534, 2002.

[57] J. Elson and D. Estrin, "Time synchronization for wireless sensor networks," in *IPDPS '01: Proceedings of the 15th International Parallel & Distributed Processing Symposium*. Washington, DC, USA: IEEE Computer Society, 2001, p. 186.

[58] M. Ding, D. Chen, K. Xing, and X. Cheng, "Localized fault-tolerant event boundary detection in sensor networks," in *Proceedings of IEEE INFOCOM*, Miami, FL, March 2005.

[59] T. Palpanas, D. Papadopoulos, V. Kalogeraki, and D. Gunopulos, "Distributed deviation detection in sensor networks," *SIGMOD Rec.*, vol. 32, no. 4, pp. 77–82, 2003.

[60] J. Staddon, D. Balfanz, and G. Durfee, "Efficient tracing of failed nodes in sensor networks," in *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*. New York, NY, USA: ACM Press, 2002, pp. 122–130

Rajkumar is native of Bidar, Karnataka, India. He received his B.E Degree in Computer Science and Engineering from VEC, Bellary, Gulbarga University Gulbarga and M.Tech in Computer Engineering from SJCE Mysore, Visvesvaraya Technological University Belgaum. and he is currently pursuing his Ph.D in Computer Science and Engineering from Visvesvaraya Technological University Belgaum, Karnataka. Presently he is serving as Assistant Professor in the department of Information Science and Engineering at Sambhram Institute Of Technology, Bangalore. His areas of interest are wireless sensor network, data analysis and security. (pyage2005@gmail.com)

Vani B. A is native of Davangere, Karnataka, India. She received her B.E Degree in Computer Science and Engineering from Bapuji Institute of Technology Davangere, Kuvempu University and M.Tech Degree in Computer Science

& Engineering from Bapuji Institute of Technology Davangere, Visveswaraiah Technological University Belgaum. Presently she is serving as Assistant Professor in the department of Information Science and Engineering at Sambhram Institute Of Technology, Bangalore. Her areas of interest are wireless communication, sensor networks. (vanignanamogh@yahoo.com)

G. Rajaraman is native of ramanathapuram, Tamil Nadu, India. He received his B.E Degree in Computer Engineering from RVS College of Engg & Technology, Dindugul, Madurai Kamaraj University, Madurai and M.Tech in Computer Science & Engineering from SASTRA University, Thanjavur. Presently he is serving as Associate Professor in the department of Information Science and Engineering at Sambhram Institute Of Technology, Bangalore. His areas of interest are wireless sensor network, system software and compiler design. (chandra1994@yahoo.co.in)

Dr. H. G. Chandrakanth is native of Bangalore, Karnataka, India. He received B.E Degree from UVCE, Bangalore University, Bangalore, India in 1991, MSEE from Southern Illinois University Carbondale, USA in 1994 and PhD from Southern Illinois University Carbondale, USA in 1998. Presently he is working as Principal in Sambhram Institute of Technology, Bangalore. (ckgowda@hotmail.com)