Security Issues and Solutions in Wireless Sensor Networks

Varsha Sahni ,Jaspreet Kaur, Sonia Sharma

Department of Computer Science and Engineering,
Guru Nanak Dev Engineering College, Ludhiana
DAV Institute of Engineering & Technology (Punjab), India

Abstract: Wireless sensor networks have gained considerable attention in the past few years. They have found application domains in battlefield communication, homeland security, pollution sensing and traffic monitoring. As such, there has been an increasing need to define and develop simulation frameworks for carrying out high-fidelity WSN simulation. In this paper, we identify the threats and vulnerabilities to WSNs and summarize the defense methods based on the networking protocol layer analysis first. Then we give a holistic overview of security issues. These issues are divided into seven categories: cryptography, key management, attack detections and preventions, secure routing, secure location security, secure data fusion, and other security issues. Along the way we analyze the advantages and disadvantages of current secure schemes in each category. In addition, we also summarize the techniques and methods used in these categories, and point out the open research issues and directions in each area.

keywords—Sensor networks, Security, Survey, key management, Attack detections and preventions, Secure routing, Secure location, Secure data aggregation, Node compromise.

I. INTRODUCTION

A Wireless Sensor Network (WSN) contain hundreds or thousands of these sensor nodes. These sensors have the ability to communicate either among each other or directly to an external base-station (BS). A greater number of sensors allows for sensing over larger geographical regions Even though sensor networks are a superset of ad hoc routing protocols, the routing protocols proposed for ad hoc routing protocols cannot be used as it is for sensor networks because of various reasons as given in [1, 2]. But surprisingly we found out that there is lack of simulation based study or research work [7] as to show why ad hoc routing protocols cannot be used in a sensor network environment. The main contribution of this paper is that we have carried out a simulation based study of ad hoc routing protocols to understand their behavior when used in a sensor network environment. The remainder of the proposal is organized as follows: Background information on WSNs including security goals, challenges, threats and attacks, and evaluation is presented in Section II. Section III gives a short summation of security issues and defense suggestions from the point of view of OSI model. Then we focus on the security issues and solutions in seven categories: cryptography, key management, attack detections and preventions, secure routing, secure location security, secure data fusion, and other security issues from Section 4 to Section 10. Finally, we summarize this paper.

II. BACKGROUND

A. Security Goals

When dealing with security in WSNs, we mainly focus on the problem of achieving some of all of the following security contributes or services:

- ***Confidentiality***: Confidentiality or Secrecy has to do with making information inaccessible to unauthorized users [9], [10]. • **Availability**: Availability ensures the survivability of network services to authorized parties when needed despite denial-of-service attacks.
- ***Integrity***: Integrity measures ensure that the received data is not altered in transit by an adversary [9], [10].
- ***Authentication***: Authentication enables a node to ensure the identity of the peer node with which it is communicating [9], [10].
- ***Non-repudiation***: Non-repudiation denotes that a node cannot deny sending a message it has previously sent.
- ***Authorization***: Authorization ensures that only authorized nodes can be accessed to network services or resources.
- ***Freshness***: This could mean data freshness and key freshness. Data freshness implies that each data is recent, and it ensures that no adversary replayed old messages.

B. Security Challenges

We summarize security challenges in sensor networks from [6], [11], [12] as follows:

- Minimizing resource consumption and maximizing security performance.
- Sensor network deployment renders more link attacks ranging from passive eavesdropping to active interfering.
- In-network processing involves intermediate nodes in end-to-end information transfer.
- Large scale and node mobility make the affair more complex.
- Node adding and failure make the network topology dynamic.

C. Threats and Attacks

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states.

Passive Attack

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active Attack

In an active attack, the attacker tries to bypass or break into secured systems.

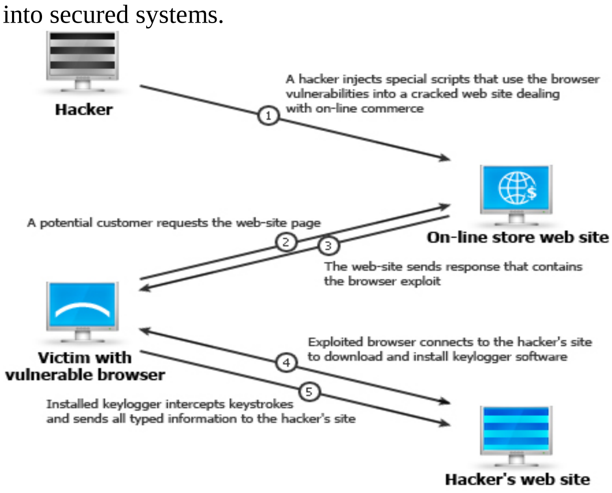
Hacker
A hacker injects special scripts that use the browser vulnerabilities into a cracked web site dealing with on-line commerce
1
On-line store web site
A potential customer requests the web-site page
2
3
The web-site sends response that contains the browser exploit
Victim with vulnerable browser
Exploited browser connects to the hacker's site to download and install keylogger software
4
5
Installed keylogger intercepts keystrokes and sends all typed information to the hacker's site
Hacker's web site

Fig 1. Active attack

This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

Distributed Attack

A distributed attack requires that the adversary introduce code, such as a Trojan horse or back-door program, to a “trusted” component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

Insider Attack

An insider attack involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task

Close-in Attack

A close-in attack involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both.

Phishing Attack

In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or paypal. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

Hijack attack

Hijack attack in a hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accident.

DoS (Denial of Service) Attack

A standard attack on the WSN that transmits radio signals which interfere with the radio frequencies used by the WSN, this is called “jamming”. An example of a DoS attack is when the base station is no longer able to answer the various queries.

Sybil Attack

An attack where the adversary is able to present more than one node identity within the network. One example of such attack is when the adversary creates multiple identities of the sensor node to generate multiple readings which result in falsification of the resulted query.

Selective Forwarding Attack:

WSNs assume that each node will accurately forward the received messages. Nevertheless, if we take security into account, a compromised node may refuse to do so. It is up to the adversary that is controlling the compromised node to either forward the received readings or not. In case of not forwarding the sensor readings, the query provided by the base station may be erroneous.

Replay Attack:

In the case of a replay attack, an attacker records some traffic patterns from the network without even understanding their content and replays them later on to mislead the base station and its query answer.

Stealthy Attack:

The adversary objective in this attack is to inject false data into the network without revealing its existence. The injected false data value leads to an erroneous query result at the base station.

Wormhole Attack:

Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

D. Evaluation

Besides implementing the security goal discussed above, the following metrics are also important to evaluate whether a security scheme is appropriate for WSNs [7], [8].

• *Resiliency*: Resilience is the ability of the network to provide and maintain an acceptable level of security service in case some nodes are compromised.

• *Resistance*: Resistance is the ability to prevent the adversary from gaining full control of the network by node replication attack in case some nodes are compromised.

•*Scalability*: self-organization and flexibility: In contrast to general ad hoc networks that do not put scalability in the first priority, designing sensor network must consider its scalability because of its large quantity of sensor nodes. Due to its deployment condition and changeable mission goals, self-organization and flexibility (such as sensor networks fusing, nodes leaving and joining, etc.) are also important factors when designing secure sensor network.

• *Robustness*: A security scheme is robust if it continues to operate despite abnormalities, such as attacks, failed nodes, etc.

• *Energy efficiency*: A security scheme must be energy efficient so as to maximize network lifetime.

• *Assurance*: It is an ability to disseminate different information at different assurance levels to the end-user. A security scheme had better allow a sensor network to deliver different level information with regard to different desired reliability, latency, etc. with different cost.

III. Attacks And Defense Suggestions In Osi Model

Here we give a short summation of security issues and defense suggestions from the point of view of Open System Interconnect (OSI) model. Using layered network architecture can help to analyze security issues, and improve robustness by circumscribing layer interactions and interfaces.

Sensor Layer model

Layered networking model of sensor network. typical layered networking model of a sensor network. Each layer is susceptible to different attacks. Even some attacks can crosscut multiple layers or exploit interactions between them. In this section, we mainly discuss attacks and defenses on the transport layer and the below layers.

A. Physical Layer

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection and modulation [5]. Jamming and tampering are the major types of physical attacks. The standard defense against jamming involves various forms of spread-spectrum or frequency hopping communication. Given that these abilities require greater design complexity and more power, low-cost and low-power sensor devices will likely be limited to single-frequency use. Other defense methods against jamming include switching to low duty cycle and conserving as much power as possible, locating the jamming area and rerouting traffic, adopting prioritized transmission schemes that minimize collisions, etc. Capturing and tampering is one of methods that produce compromised nodes. An attacker can also tamper with nodes physically, interrogate and compromise them. Tamper protection falls into two categories: passive and active [11]. Passive mechanisms include those that do not require energy and include technologies that protect a circuit from being detected (e.g., protective coatings, tamper seals). Active tamper protections involve the special hardware circuits within the sensor node to prevent sensitive data from being exposed. Active mechanisms will not be typically found in sensor nodes since these mechanisms add more cost for extra circuitry and consume more energy. Instead, passive techniques are more indicative of sensor node technology.

B. Data Link Layer

The data link layer or media access control (MAC) is responsible for the multiplexing of data streams, data frame detection, medium access and error control [5]. It provides reliable point-to-point and point-to-multipoint connections. in a communication network, and channel assignment for Neighbor-to-neighbor communication is a main task for this layer. Collision, exhaustion, and unfairness are major attacks in this layer. Error-correcting code can ease collision attack; however, the result is limited because malicious nodes can still corrupt more data than the network can correct. Also, the collision-detection mechanism cannot completely defend against that attack because proper transmission still need cooperation among nodes and subverted nodes could intentionally and repeatedly deny access to the channel, expending much less energy than in fulltime jamming . TDMA is another method in preventing collisions. But it requires more control resources and is still susceptible to collisions. Adversaries can let sensor nodes execute a large number of tasks to deplete the battery of these nodes. This exhaustion attack will compromise the system availability even if the adversary expends few efforts. Random back–offs only decrease the probability of an inadvertent collision, thus they would be ineffective at preventing this attack. Time-division multiplexing gives each node a slot for transmission without requiring arbitration for each frame. This approach could solve the indefinite postponement problem in a back–off algorithm, but it is still susceptible to collisions. A promising solution is rate limiting in MAC admission control, but it still needs additional work.

C. Network Layer

Sensor nodes are scattered in a field either close to or inside the phenomenon [5]. Special multihop wireless routing protocols between the sensor nodes and the sink node are needed to deliver data throughout the network. Karlof and Wagne summarize the attacks of the network layer as follows: Spoofed, altered, or replayed routing information; Selective forwarding; Sinkhole attacks; Sybil attacks; Wormholes; HELLO flood attacks; and acknowledgement spoofing.

- **Countermeasure summary in Network layer**

Encryption and authentication, multipath routing, identity verification, bidirectional link verification, and authentication broadcast can protect sensor network routing protocols against external attacks, bogus routing information, Sybil attacks, HELLO floods, and acknowledgement spoofing. Sinkhole attacks, and wormholes pose significant challenges to secure routing protocol design, especially integrating node compromise. It is unlikely to find effective countermeasures against these attacks that can be applied after deployment. It is crucial to design routing protocols in which these attacks are meaningless or ineffective. Geographic routing protocols are one class of protocols that holds promise.

D. Transport Layer

The transport layer protocols provide reliability and session control for sensor node applications [5]. This layer is especially needed when the system plans to be accessed through Internet or other external networks. Though it is considered to have few security issues in this layer, there are still some types of attacks, such as flooding and desynchronization that can threaten the security. Though limiting the number of connections can prevents flooding, it also prevents legitimate clients from connecting to the victim as queues and tables filled with abandoned connections. Protocols that are connectionless, and therefore stateless, can naturally resist this type of attack somewhat, but they may not provide adequate transport-level services for the network. Solving client puzzles can partially ease this type of attack. Desynchronization can disrupt an existing connection between two endpoints. In this attack, the adversary repeatedly forges messages carrying sequence numbers or control flags, which cause the endpoints to request retransmission of missed frames to one or both endpoints. One counter to this attack is to authenticate all packets exchanged, including all control fields in the transport protocol header. The endpoints could detect and ignore the malicious packets, supposing that the adversary cannot forge the authentication message.

IV. CRYPTOGRAPHY

A. State-of-the-Art

Cryptography is the basic encryption method used in implementing security. Symmetric key cryptography uses the same key for encryption and decryption. Another type of encryption method, asymmetric or public key cryptography uses different keys to encrypt and decrypt. On one hand, asymmetric key cryptography (e.g., the RSA signature algorithm) requires more computation resources than symmetric key cryptography (e.g., the AES block cipher) does, on the other hand, symmetric key cryptography is difficult for key deployment and management. Cryptographic methods used in WSNs should meet the constraints of sensor nodes and be evaluated before choosing. In this section, we focus on cryptography evaluations and cryptography architectures.

1) Cryptography Evaluations: To evaluate the computational overhead of cryptographic algorithms, Ganesan in chose RC4, IDEA, RC5, MD5 and SHA1 as the popular symmetric encryption and hashing function schemes. They did a series performance evaluation experiments for these choosing algorithms based on different hardware platforms including Atmega 103, Atmega 128, M16C/10, SA-1110, PXA250 and UltraSparc2.

V. KEY MANAGEMENT

A. State-of-the-Art

Considering security, key management is very important and complex especially in symmetric cryptography structure. Sensor network dynamic structure, easy node compromise and self organization property increase the difficulty of key management and bring a broad research issues in this area. Due to the importance and difficulty of key management in WSNs, there are a large number of approaches focused on this area. Based on the main technique that these proposals used or the special structure of WSNs, we classify the current proposals as key pre-distribution schemes, hybrid cryptography schemes, one way hash schemes, key infection schemes, and key management in hierarchy networks, though some schemes combine several techniques.

1) Key Pre-Distribution Schemes: In the key predistribution schemes, sensor nodes store some initial keys before they are deployed. After deployed, the sensor nodes can use the initial keys to setup secure communication. This method can ease key management especially for sensor nodes that have limited resource. Thus many approaches adopt key pre-distribution method. In addition, in these approaches, the communications between the base station and sensors are smaller compared with centralized approaches, thus the base station is not a bottleneck problem. So, we not only call it key pre-distribution management, but also distributed key management. A naive solution is to let all the nodes to carry a master secret key. Any pair of nodes can use this global master secret key to initiate key management. The advantage of this scheme is that it only needs store one master key in a node before its deployment.

- **Determinate schemes**

Contrary to probability schemes, some of approaches guarantee that any two intermediate nodes can share one or more predistribution keys. We call this type of schemes as determinate schemes.

2) Hybrid Cryptography Schemes: Though most framework use one type of cryptograph, there still exist some schemes that use both asymmetric-key and symmetric-key cryptographs. For example, a hybrid scheme proposed by Huang, et al. in balances public key cryptography computations in the base station side and symmetric key cryptography computation in sensors side in order to obtain adorable system performance and facilitate key management. On one hand, they reduce the computation intensive elliptic curve scalar multiplication of a random point at the sensor side, and use symmetric key cryptographic operations instead. On the other hand, it authenticates the two identities based on elliptic curve implicit certificates, solving the key distribution and storage problems, which are typical bottlenecks in pure symmetric-key based protocols.

3) One Way Hash Schemes: To ease key management, many approaches use the one-way key method that comes from one-way hash function technique. For example, Zachary [50] propose a group security mechanism based on one-way accumulators that utilizes a pre-deployment process, quasicommutative property of one-way accumulators and broadcast communication to maintain the secrecy of the group membership. Another group security mechanism proposed by Dutta, in also use one-way function to ease group node joining or revocation. Their scheme has self-healing feature, a good property that makes the qualified users recover lost session keys over a lossy mobile network on their own from the broadcast packets and some private information, without requesting additional transmission from the group manager. The one-way hash function can also adapt to conduct public key authentication. For example, Du, et al. use all sensors' public keys to construct a forest of Merkle trees of different heights, and by optimally selecting the height of each tree, they can minimize the computation and communication costs. To ease the joining and revocation issues of membership in broadcast or group encryption, many approaches use predistribution and/or a local collaboration technique. For example, RBE (Randomized Broadcast Encryption scheme), proposed by Huang and Du in, uses a node-based key predistribution technique. Besides predistribution future group keys, the group rekeying scheme of Zhang and Cao also adopts the neighbors' collaboration.

4) Key Infection Schemes: Contrary to most of key management using pre-loaded initial keys, Anderson, et al. propose a key infection mechanism. In a key infection scheme,different from key pre-distribution schemes, no predistribution key is stored in sensor nodes. This type of schemes establishes secure link keys by broadcasting plaintext information first. This type of schemes is not secure essentially. However, Anderson, et al. show that their key infection scheme is still secure enough for non-critical commodity sensor networks after identifying a more realistic attacker model that is applicable to these sensor networks. Their protocol is based on the assumption that the number of adversary devices in the network at the time of key establishment is very small (in their results, less than 3% of the devices are adversaries).

Similar to scheme in,Miller and Vaidya in propose a predistribution scheme that allows neighboring sensors to establish secure link keys from plaintext keys that are broad cast by sensors in their neighborhood. Their scheme has better security performance than by utilizing a special property of hardware - multiple channels available on some sensor hardware, and spatial diversity of device locations.

5) Key Management in Hierarchy Networks: Though many key management approaches are based on a normal flat structure, there are still some approaches that utilize a hierarchical structure in order to ease the difficulties by balancing the traffic among a command node (base station), Gateways, and sensors. These are the three parts of networks that have different resources. In this type of key management, some use the physical hierarchical structure of networks such as, while others implement their hierarchy key management logically in physical flat structure sensor networks, which only include a base station and sensors. For example, LKHW (Logical Key Hierarchy for Wireless sensor networks), proposed by Pietro, et al. in,integrates directed diffusion and LKH (Logical Key Hierarchy) where keys are logically distributed in a tree rooted at the key distribution center (KDC). A key distribution center maintains a key tree that will be used for group key updates and distribution, and every sensor only stores its keys on its key path, i.e. the path from the leaf node up to the root. In order to efficiently achieve confidential and authentication, they apply LKHW: directed diffusion sources are treated as multicast group members, whereas the sink is treated as the KDC.

VI. Attack Detections And Preventions

A. State-of-the-Art

Security issues mainly come from attacks. If no attack occurred, there is no need for security. Detecting and defending against attacks are important tasks of security mechanisms. Attacks in WSNs are classified as external attacks and internal attacks. Compared with external attacks, internal attacks are hard to be detected and prevented. Thus, besides introducing some normal attack detecting mechanisms, we also describe some special node compromise detecting methods. Fig. 2 shows the taxonomy.

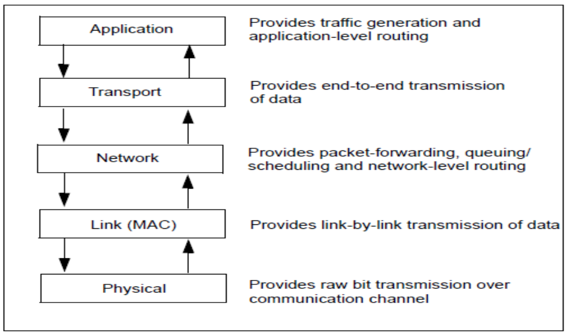
Application
Provides traffic generation and application-level routing
Transport
Provides end-to-end transmission of data
Network
Provides packet-forwarding, queuing/ scheduling and network-level routing
Link (MAC)
Provides link-by-link transmission of data
Physical
Provides raw bit transmission over communication channel

Fig 2: Taxonomy

1) Attack Detecting and Prevention Mechanisms:

• **Normal external attack defenses**

Currently, there are some approaches that are focus on external attacks, described as the following:

• **Sybil attack**: Newsome, et al. in [15] establish taxonomy of the Sybil attacks (A Sybil attack occurs when a single node illegally claims multiple identities to other nodes in the network) by distinguishing different attack types and proposing several methods to identify these attacks, including radio resource testing, key validation for random key predistribution, position verification, and registration.

• **Wormhole attack**: In a wormhole attack, an adversary tunnels messages received in one part of the network over a low-latency link and replays them in a different part to make a fake that these two parts are very close. Normally, wormhole attacks need two distant colluding malicious nodes to communicate directly through relaying packets along an out-of-bound channel available only to the attackers. Hu, et al. present a mechanism, packet leashes, for detecting and thus defending against wormhole attacks, and a specific efficient authentication protocol, TIK(TESLA with Instant Key disclosure), that implements leashes. A leash is any information that is added to a packet and is designed to restrict the packet's maximum allowed transmission distance. They distinguish between a geographical leash, which ensures that the recipient of the packet is within a certain distance from the sender, and a temporal leash, which ensures that the packet has an upper bound on its lifetime. The latter restricts the maximum travel distance, since the packet can travel at most at the speed of light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect whether the packet traveled further than the leash allows. Wang and Bhargava propose a mechanism, MDS-VOW (Multi-Dimensional Scaling – Visualization of Wormhole), to detect wormholes by using multi-dimensional scaling to reconstruct the layout of the sensors and adopting a surface smoothing scheme to compensate the distortions caused by distance measurement errors.

• Node replication attack: It can be detected by Randomized Multicast and Line-Selected Multicast. Randomized Multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes, while Line-Selected Multicast uses the topology of the network to detect replication nodes.

• Jamming attack: Li, et al. in study controllable jamming attacks in WSNs, which are easy to launch and difficult to detect and confront. They derive optimal strategies or policies for both jammer and the network defense system under two cases: perfect knowledge of the jammer and the defense system, lack of knowledge of the attacker and the network.

• **Attack/failed node detection**

As a whole, most attack detecting methods can be classified as centralized approaches or neighbors' cooperative approaches.

• Centralized approaches: The type of method uses the base station to detect attacks. Although the schemes in are mainly used to diagnose failed nodes, the idea can also be adapted to detect attacks. In the approach of sensor networks are diagnosed by injecting queries and collecting responses. To reduce the large communication overhead, which results in failure detection latency, their solution reduces the response implosion by sacrificing some accuracy. Staddon, et al. in propose another centralized approach to trace the failed nodes. Nodes append a little bit of information about their neighbors to each of their measurements and transmit them to the base station to let the latter know the network topology. Once the base station knows the network topology, the failed nodes can be efficiently traced using a simple divide&conquer strategy based on adaptively routing update messages.

Denial of service attack and countermeasures

Denial of service (DoS) means that the adversaries attempt disrupting, subverting, or destroying sensor networks in order to diminish or eliminate its capacity to perform its expected function. DoS can disrupt sensor nodes, communications among nodes, and the base station to implement their goal, which is disabling sensor network availability. Draining the battery by repeating service request attacks, benign repeating energy-hungry tasks, or repeating malignant burden tasks is also a special type of DoS. Denial-of-Message attack is another type of DoS in which adversaries deprive other nodes from receiving broadcast messages. To prevent DoS attacks, we can adopt the following methods:

• Watchdog and Reputation Rating based scheme: Marti, et al. in propose a watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. The Watchdog Scheme is further investigated and extended to Reputation Rating Scheme. In the Reputation Rating Scheme the neighbors of any single node collectively rate the node according to how well the node executes the functions requested of it. Compared to malicious nodes disrupting the network, selfish nodes only refuse to perform any function requested by the others, such as packet forwarding, to save energy. Reputation Rating Scheme conquers the selfish nodes by giving them a bad strike.

• Virtual currency: Virtual currency systems use credit or micro payments to compensate for the service of a node. A node receives a virtual payment for forwarding the message of another node, and this payment is deducted from the sender (or the destination node). Two examples of such systems are: Nuglets and Sprite .Nuglets has two models: Packet Purse Model and Packet Trade Model. In the Packet Purse Model, each packet is loaded with enough Nuglets by the source, and each forwarding host takes out some Nuglets for its forwarding service. The advantage of this approach is that it discourages users from flooding the network. In the Packet Trade Model, packets are traded for Nuglets by the intermediate nodes. The direct advantage of this method is that the source does not need to know how many Nuglets need to be loaded into the packet. To prevent illegal manipulation of the nodes' Nuglets, tamper-proof hardware is required at each node to store all the relevant IDs, Nuglets counter, and cryptographic materials. Sprite a simple, cheat-proof, credit-based system uses credit to provide incentives for mobile nodes to cooperate and report actions honestly. The basic idea of this scheme is as follows: a system has a Credit Clearance Service (CCS) to determine the charge and credit to each node involved in the transmission of a message. Payments and charges are determined from a game theory perspective.In this scheme, the sender is charged to prevent a denialof-service attack to the destination by sending it a lot of traffic. A node receives credit only when the next node on the path reports a valid receipt to the CCS to acknowledge the successful transmission.

1) Special Node Compromise Detecting Mechanisms:

Although many node compromise detecting mechanisms use centralized detecting methods or neighbors' cooperative/ localized methods to monitor the activities of nodes, there are still some mechanisms use code testing methods and a special scheme uses location verification method.

• **Code testing schemes**

In the context of node compromise code testing schemes in WSNs, some implement their schemes by software-based, while others use hardware to assist their mechanisms.

• Software-based approach: In software-based approaches, such as , rely on optimal program code and exact time measurements. These approaches enable software-based attestation by introducing an optimal program verification process that verifies the memory of a sensor node by calculating hash values of randomly selected memory regions.

• Hardware-based approach: Normal hardware-based approaches such as are based on public-key cryptography and require extensive computational power, as well as the transmission of large messages, making these approaches not usable in WSNs. Krauss, et al. suppose that some cluster nodes posses much more resources than the majority of clusters and are equipped with a Trusted Platform Module in the hybrid WSNs.Their hardware-based attestation protocols use the nodes equipped with Trusted Platform Module as trust anchors and can enable attestation with more efficiently. However, their mechanisms can only make sense in Hybrid WSNs.

• **Location verification schemes**

Song, et al. in provide a method to detect node compromise by comparing the previous position of nodes with current position. The main idea of their mechanism is based on the assumption that a node compromise often consists of three stages: physically obtaining and compromising the sensors, redeploying the compromised sensors, and compromised nodes launching attacks after their rejoining the network. In some applications an attacker may not be able to precisely deploy the compromised sensors back into their original positions. Their mechanism can detect compromise events when compromised nodes change positions or identities. But sometimes adversaries can compromise the nodes by communicating them, breaching their security mechanism, and controlling them without physically touching them or moving their positions. Under such condition, their mechanism will not detect the compromise events.

VII. SECURE ROUTING

A. State-of-the-Art

WSNs use multi-hop routing and wireless communication to transfer data, thus incur more routing attacks. There are a lot of approaches to ease routing security. In this section, we review existing secure routing approaches.

1) Secure Routing Protocols for Ad Hoc Networks: Because WSNs came from ad hoc, some of secure routing algorithms in the latter are still valued to be reviewed though they may have difficulty to be suited to sensor networks. Some secure AODV algorithms that may be adapted in WSNs have some effects on defending against external attacks because they suggest secure routing information. These security mechanisms still meet security issues when the nodes are compromised and the security information such as key is disclosed to the attackers. A certificate approach, URSA, a ubiquitous and robust access control solution proposed by Luo, et al. in , uses the multiple nodes decision to certify/revoke a ticket to ensure access control service ubiquity and resilience. Sanzgiri, et al. in also propose a secure routing protocol based on certificate. Their protocol, Authenticated Routing for Ad hoc Networks (ARAN), works to defend against identified attacks under such a scenario where no network infrastructure is predeployed, but a small amount of prior security coordination is expected before deployment.

2) Multi-Path Routing: Some approaches use multi-path routing and neighbor collaboration techniques, such as Multi-path routing, location disguise, and relocation methods can be used to protect base stations In the environment where the network only has a small number of compromised nodes, Multi-path schemes provide more reliable routing, though they introduce more communication overheads. However, in the environment where the network has a large number of compromised nodes, if the compromised can modify the routing data, system may involve more security issues.

3) Secure Routing for Cluster or Hierarchical Sensor Networks:

Some researchers utilize the special structure in physical or logical cluster or hierarchical sensor networks in order to provide more efficient secure routing algorithms. For example, Tubaishat, et al. in propose an energy efficient level based hierarchical system. In their approach, they divide the sensor nodes into different levels. The lower-level sensor nodes only sense and disseminate data, whereas the higherlevel sensors find the shortest path to the sink node and aggregate data in addition to forwarding it. A sensor becomes a cluster head and is valued as level 2 if it has the highest number of neighbors (NBR). Sensors are initiated at level 0 when embedded in the network. The incremental level depends on a sensor's reliability and its energy consumption. When a sensor finds its neighbors it upgrades itself to level 1 and then to level 2 if it becomes a cluster head. A sensor connected to two or more cluster heads upgrades itself to level 3 (they call this node the root). Based on the level classifications, they propose a new routing protocol algorithm that depends on the number of neighbors and their levels to disseminate the queries and data. The level-based hierarchical routing protocol compromises between shortest path and energy consumption. Based on the usage of hierarchical structure of sensor networks and symmetric key, they propose a secure routing protocol. In addition, they propose a group key management scheme which every sensor node contributes its partial key for computing the group key.

VIII. SECURE LOCATION

A. State-of-the-Art

Location information is very important in some applications of sensor network, such as reconnaissance of opposing forces. Many monitoring applications require near accurate position besides event self. Besides this type of application, many routing protocols or other security mechanisms also need location information or distance information among neighbor nodes. Thus, providing secure and reliable location information in some special applications under adversaries' attacks need pay more attention.

1) Secure Location Scheme With Beacons: In some location systems, some sensors have a position system such as GPS to locate their positions. We call this type of sensors beacon nodes. These location systems use location information from these beacon nodes and some positioning and ranging techniques to construct the whole location systems. Positioning and ranging techniques in wireless networks mainly rely on measurements of the times of flight of radio or ultrasound signals, and on the measurements of received strengths of radio signals of devices. However, these methods are highly vulnerable to attacks from dishonest nodes and external attackers.

IX. OTHER SECURITY ISSUES

A. State-of-the-Art

Other security issues include security-energy assessment, data assurance, survivability, etc. It's very important to study these areas due to a sensor network's special character, such as battery limitation, high failure probability nodes, easier compromised nodes, unreliable transmission media, etc.

1) Security-Energy Evaluation: As to our knowledge, few research works have been done in this area. To evaluate the relation between energy and security, Law, et al. in describe an assessment framework based on a system profile after carefully reviewing the dominant issues of energy security trade-off in the network protocol and key management design space.

2) Information Assurance: Due to resource limitations of a sensor network, the transmission all of information with the same reliability requires more resources and is impractical. For the user, different types of events have different levels of importance. Based on this assumption, Deb, et al. in propose an assurance level mechanism to transmit the information of different criticality with different reliability (probability to sink) using hop-by-hop broadcast.

3) Survivability Evaluation: As so far, many schemes are proposed to secure WSNs, it is crucial to build a model to evaluate these schemes with regard to survivability of a WSN. In Li, et al. propose a quantitative evaluation model for a typical pre-distribution key management scheme. Their survivability evaluation model includes three major attributes: resilience, resistance, and robustness. Based on their model, they show that that increasing the key space and decreasing the multiple key space would improve the survivability of WSNs. Kim, et al. in propose a survivability model with software rejuvenation methodology, which is applicable in security field and also less expensive. Based on their model, they analyze each cluster of a hierarchical cluster based WSN as a stochastic process based on semi-Markov Process (SMP) and Discrete-Time Markov Chain (DTMC). Different from other approaches considering node survivability, Kumar, et al. in simulate a DoS attack on a WSN-gateway (Most approaches denote it as the base station) of a WSN to highlight how the computing resource of the gateway can be exhausted which directly hampers or disables the data collection efforts. Skelton, et al. in survey the issues and concerns surrounding the deployment and maintenance of WSNs. Their research focuses on several distinct areas affecting survivability: 1) power, 2) network/node destruction and repair, and 3) network security. They summarize that the two distinct categories of survivability: information access and end-to-end communication, are applied to all of the networking layers. Based these two requirement categories, they examine the cause of WSN failure, both hardware and software based, and then identify means by which survivability may be supported.

4) Trust Evaluation: Sun, et al. in presents a framework for trust evaluation in distributed networks. They address the concept of trust in computer networks, develop trust metrics with clear physical meanings, develop fundamental axioms of the mathematical properties of trust, and build trust models that govern trust propagation through third parties. Further, they identify some attacks that can reduce the effectiveness of trust evaluation, and develop some techniques to defend against these attacks. Then, they design a systemic trust management system. Their framework can be used to assist route selection and malicious node detection. Crosby, et al. in describes a reputation based trust framework with a mechanism for the election of trustworthy cluster heads in cluster based WSNs. Their cluster formation algorithm establishes trusted clusters by the help of pre-distributed keys.

X. SUMMARY

Security in sensor networks is a new area of research, with a limited, but rapidly growing set of research results. Because of its linchpin in some application areas, it is worth studying. In this paper, we present a nearly comprehensive survey of security researches in wireless sensor networks, which has been presented in the literature.

We summarize security challenges and analyze threats and attacks. Based on the network protocol model, we review nearly all types of crippling attacks against the functions of protocol layers. We also provide summarization of countermeasures and design considerations. Then we review seven major issues in securing WSNs and also proposed our suggestions:

- Cryptography: Cryptography Selection is fundamental to providing security services in WSNs. Most security approaches adopt symmetric key cryptography, thus introducing complex key management. Although some recent studies show public key cryptography is available for WSNs, private key operations in asymmetric cryptography schemes are still too expensive in terms of computation and energy cost for sensor nodes, and still need further studies.
- Key management: Key management is the linchpin of cryptograph mechanism especially for symmetric key cryptography. After reviewing current approaches, we give our suggestions: adopting symmetric cryptography and one-way hash functions and using a distributed mechanism instead of a centralized mechanism; combining deployment knowledge, location information, and key pre distribution; integrating node identity and key produce; adopting an adaptive re-key mechanism to defend against cryptography attacks; integrating secure resilience and a system application environment; considering network structure, etc.
- Attack detections and preventions: Although most secure schemes are able to limit the effects of attacks, attack detections are still need for system security. In general, most attack detecting mechanisms belong to centralized approaches or neighbors' cooperative approaches. The disadvantage of the first method is that it introduces more routing traffic from the given node to the base station; while the second method introduces more computing process and monitoring tasks for neighbor nodes. In all, Watchdog and Reputation Rating based or Virtual currency methods are able to prevent DoS attacks in some extent. Code testing methods and location verification methods open our eyes to node compromise detection, though they need improvement.
- Secure routing: Many sensor network routing protocols are quite simple and offer little to no security features, and there are some types of attacks that disable routing.

Though there are some secure routing protocols for adhoc networks, figuring out how to adapt them to sensor networks still needs more works. After reviewing current Approaches, we give our suggestions: Authentication is required for broadcast; A system should prevent adversaries from knowing the network topology; Multi-path can tolerate routing attacks to some extent; Routing information should be encrypted; Identifying malicious nodes and isolating them from routing path will improve system security performance; Integrating location information can help a routing path immune spoof; Using localized algorithms instead of centralized ones will improve system performance; Using the special structure of cluster or hierarchical sensor networks can provide more efficient secure routing algorithm; Base station protection needs more considerations; Reduce overhead when possible.

- Security location: Providing reliable and accurate location or position information is the key factor in some sensor networks when position or location information is the object of these networks, or if they use distance or geography routing algorithms. To provide location security, we can adopt multiple verifications to detect or tolerate attacks in beacon detecting location mechanisms. In a group membership estimating location mechanism, we can use the statistical method and deployment knowledge to secure location.
- Secure data fusion: Data fusion security issues can occur in the original sensors, intermediate nodes, and the aggregators.

To provide security, we can adopt authentication, neighbor nodes' collective endorsement or similar methods to verify the correction of the aggregation reports or we can use statistical methods to filter the fake data. Some studies suggest that using ciphertext instead of plaintext to prevent the disclosure of data in intermediate nodes, though these methods usually lower the security level.

- Other security issues: Security assessment, data assurance, survivability, trust evaluation, end-to-end security, security and privacy support, node compromise distribution,etc. are also important in sensor network security .Until now, there have been only a few approaches available, and more studies are needed in these areas .As our survey shows, there are several unsolved research problems that deserve more attention:
- Inexpensive private key operations on sensor nodes: Though some studies show that asymmetric key cryptography can be used to secure WSNs, improving the efficiency of private key operations on sensor nodes is highly desirable.

• Key management for mobile flat WSNs: Most current key management protocols are only suitable for static WSNs.

New protocols for mobile WSNs including mobile nodes and mobile base stations need to be developed.

•Intelligent attack/node compromise detecting mechanism:

Most current detecting systems monitor all the nodes in the system without emphasis, and the system should decentralize their resources evenly in all nodes in order to monitor whether they have larger compromise probabilities or not. That makes the detecting mechanism less efficient. Due to the heavy work, the system performance may decrease largely, and may even make this work unpractical. It is highly desirable to design an efficient and effective mechanism that chooses those nodes with larger probabilities of being attacked as the main monitoring objects.

• Secure routing for mobile WSNs: Most current secure routing algorithms assume the sensor network is stationary. It is highly needed to study secure routing protocols for mobile WSNs.

• Secure routing to defend against undetected attacks: Currently, there are some protocols that let routing paths bypass the detected compromised nodes or attacks. However, most compromise activities can not be immediately detected because any detecting mechanism needs time and the fraudulent action of adversaries (adversaries don't want system to notice their attacking activities, thus they will adopt any action that one can imagine to make the detecting time longer.) makes the time even longer. Consequently, current secure routing algorithms have no effect to conquer undetected attacks. New secure routing protocols that can defend against undetected attacks or node compromise are highly desirable.

• Security and QoS: Most current security studies focus on individual topics of security issues. However, security overhead will degrade other performances of WSNs. The Trade off between security and QoS needs to be evaluated.

• Base station protection: Most approaches assume thebase station is secure and robust enough. However, in some special application environment, such as battlefield surveillance, base stations may be easy to be destroyed or attacked. Under such conditions, base station protection and the other issues that are introduced by the base station protection must be carefully investigated.

References

[1] I. Akylidiz, W. Su, Sankarasubramaniam, and E.Cayrici, "A survey on sensor networks", IEEE Communications Magazine, Volume: 40 Issue: 8, August 2002, pp.102-114.

[2] K. Akkaya and M. Younis, "A survey of Routing Protocols in Wireless Sensor Networks", Elsevier Ad Hoc Network Journal, 2005, pp 325-349.

[3] C.Perkins, E.B.Royer and S.Das,"AdHoc On-Demand Distance Vector (AODV) Routing", RFC 3561, IETF Network Working Group, July 2003.

[4] E.M.Royer and C.K.Toh, " A Revisew of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, April 1999, pp. 46-55.

[5] W.R.Heinzelman, A. Chandrakasan and H.Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", IEEE Proc. Hawaii Int'l Conference. Jan 2000, pp 1-10.

[6] J. Heidemann and N. Bulusu et al., " Effects of detail in wireless network Simulation", In Proceedings of the SCS Multiconference on Distributed simulation", January 2001, pp 3-11.

[7] Bertocchi, F et.al, "Performance Comparison of Routing Protocols for Ad hoc networks", In proceedings of Global Telecommunications Conference, 2003, pp 1033-1037.

[8] H. Jiang and J. Garcia-Luna-Aceves,"Performance comparison of three routing protocols for ad hoc networks", In Proceedings of IEEE ICCCN 2001.

[9] http://www.red3d.com/cwr/boids/

[10] Gowrishankar. S, T.G. Basavaraju, SubirKumarSarkar," Issues in Wireless Sensor Networks", In proceedings of the 2008 International Conference of Computer Science and Engineering, (ICCSE 2008), London, U.K., 2-4 July, 2008.

[11] Bai, Fan; Helmy, Ahmed (2006). A Survey of Mobility Models in Wireless Adhoc Networks. (Chapter 1 in Wireless Ad-Hoc Networks. Kluwer Academic. 2006).

[12] I. Akylidiz, W. Su, Sankara subramaniam, and E.Cayrici, "A survey on sensor networks", IEEE Communications Magazine, Volume: 40 Issue: 8, August 2002, pp.102-114.

[13] K. Akkaya and M. Younis, "A survey of Routing Protocols in Wireless Sensor Networks", Elsevier Ad Hoc Network Journal, 2005, pp 325-349.

[14] C.Perkins, E.B.Royer and S.Das,"AdHoc On-Demand Distance Vector (AODV) Routing", RFC 3561, IETF Network Working Group, July 2003.

[15] E.M.Royer and C.K.Toh, " A Revisew of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, April 1999, pp. 46-55.

[16] Information Sciences Institute, "The Network Simulator Ns-2", Http://www.isi.edu/nanam/ns/, University of Southern California.

[17] NRL's Sensor Network Extension to NS-2,Http://www.nrlsensorsim.pf.itd.nrl.navy.mil/.

[18] W.R.Heinzelman, A. Chandrakasan and H.Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", IEEE Proc. Hawaii Int'l Conference. Jan 2000, pp 1-10.

[19] J. Heidemann and N. Bulusu et al., " Effects of detail in wireless network Simulation", In Proceedings of the SCS Multiconference on Distributed simulation", January 2001, pp 3-11.

[20] Stuart Kurkowski, Tracy Camp and Michael colagrosso,"MANET Simulation Studies: The Incredibles", Special Issue on Medium Access and Call Admission Control Algorithms for Next generation Wireless Networks", volume 9, Issue 4, October 2005.

[21] Karlof C. and Wagner D. (1996), " Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley, Funded in part by DARPA NEST Proceedings of ECMAST, Vol. 26, Issue no. 4, pp. 129- 148.