SENSOR NETWORK SECURITY

Divya Atri Prarthana Kumari[1], Ms. Indu[2]
[1]Student, [2]Assistant Professor
Department of Computer Science Engineering, BMCEM, Sonipat

Abstract: Wireless sensor networks (WSNs) use small nodes with constrained capabilities to sense, collect, and disseminate information in many types of applications. As sensor networks become wide- spread, security issues become a central concern, especially in mission-critical tasks. 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, Ad hoc networks, Survey, key management, Attack detections and preventions, Secure routing, Secure location, Secure data aggregation, Node compromise.

I. INTRODUCTION

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[1]:

•Confidentiality: Confidentiality or Secrecy has to do with making information inaccessible to unauthorized user. A confidential message is resistant to revealing
its meaning to an eavesdropper.

•Availability: Availability ensures the survivability of network services to authorized parties when needed despite denial-of-service attacks. A denial-of-service attack could be launched at any OSI (Open System Interconnect) layer of a sensor network.

•Integrity: Integrity measures ensure that the received data is not altered in transit by an

•Authentication: Authentication enables a node to ensure the identity of the peer node with which it is communicating

•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. Since all sensor networks provide some forms of time varying measurements, we must ensure each message is fresh. Data freshness implies that each data is recent, and it ensures that no adversary replayed old messages. Moreover, as new sensors are deployed and old sensors
fail frequently in WSNs, the following forward and backward secrecy are also important to security:

•Forward secrecy: a sensor should not be allowed to know future messages after it leaves the network.

•Backward secrecy: a newly joining sensor should not be able to know any previously transmitted message.

B. Security Challenges

We summarize security challenges in sensor networks from as follows:[3][6]

• 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.

• Wireless communication characteristics render traditional wired-based security schemes unsuitable.

• Large scale and node mobility make the affair more complex.

• Node adding and failure make the network topology dynamic.

C. Threats and Attacks

Security issues mainly come from attacks. Base stations in WSNs are usually regarded as trustworthy. Most research studies focus on security issues among sensor nodes[6].[9] [12]If no attack occurred, there is no need for security. Generally, the attack probability within sensor networks is larger than that of any other types of networks, such as wireless LANs, due to their deployment environments and resource limitations.These attacks can be classified as external attacks and internal attacks. In an external attack, the attacker node is not an authorized participant of the sensor network . External attacks can further be divided into two categories: passive and active. Passive attacks involve unauthorized ‘listening’ to the routing packets. This type of attack can be eased by adopting different security methods such as encryption. Active external attacks disrupt network functionality by introducing some denial-of-service (DoS) attacks, such as jamming, power exhaustion. Authentication and integrity will ease most active external attacks except jamming. The standard defense against jamming involves various forms of spread-spectrum or frequency hopping communication. 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 scheme that minimize collisions, etc. Node compromise is the major problem in sensor networks that leads to internal attacks.

With node compromise, an adversary can perform an internal attack. In contrast to disabled nodes, compromised nodes actively seek to disrupt
or paralyze the network. Normally, compromised nodes can be obtained by the following methods:

• Attackers capture sensor nodes and reprogram them. The advantage of this method is quick and easy. But this method has some limitations. Firstly, it is not easy to
capture and reprogram sensor nodes automatically. Most time, attackers must manually capture nodes and reprogram them. Secondly, in some applications, the deployment environment makes it difficult or even impossible for attackers to capture sensor nodes, e.g. some military applications. Thirdly, WSNs can locate the compromised nodes by monitor node activity, location, etc.

• Attackers can deploy nodes with larger computing resources such as laptops to attack sensor nodes. For example, laptop attackers' nodes can communicate sensor nodes, breach their security mechanisms, insert malicious codes and make them as compromised nodes without physically touching them or moving their positions. These laptop nodes compromising activities can execute at all time, and these compromise activities are hard to be detected, and can be implemented automatically. The disadvantage is that attackers need some time to breach security mechanisms of sensor nodes.

• Attackers can deploy big nodes as compromised nodes. Attackers can deploy big nodes such as laptop nodes as compromised nodes to replace current sensor nodes when they get the secret information by attacking normal nodes. Similar to the above case, it is hard for detecting mechanisms to detect such compromised nodes. The disadvantages of this method are: attacking time is a little longer compared with the first introduced method; the cost is expensive when using one laptop as one node. Someone may say that attacker can use one laptop to forge several nodes. This type of attack is Sybil attack System can easily locate them by using Location Verification, Identity Verification. Compared with external attacks, internal attacks are hard to be detected and prevented, thus raising more security challenges. Compromised nodes can do the following attacks:

• Compromised node can steal secrets from the encrypted data which passed it;

• Compromised node can report wrong information to the network;

• Compromised node can report other normal nodes as compromised nodes;

• Compromised node can breach routing by introducing many routing attacks, such as selective forwarding, black hole, modified the routing data, etc., while systems are hard to notice these activities, and normal encryption methods have no effect to prevent them because they own the secret information such as keys.

• Compromised nodes may exhibit arbitrary behavior and may collude with other compromised nodes.

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

• 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.

II. ATTACK AND DEFENCE SUGGESTION 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[4]. Using layered network architecture can help to analyze security issues, and improve robustness by circumscribing layer interactions and interfaces. Figure 1 is the 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.

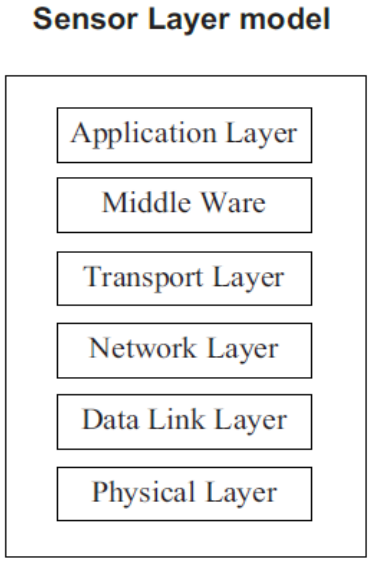

Fig. 1. Layered networking model of sensor network.

III. CRYPTOGRAPHY

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[5].

1) Cryptography Evaluations*:* To evaluate the computational overhead of cryptographic algorithms, Ganesan, et al. in chose RC4, IDEA, RC5, MD5 and SHA1 as the popular symmetric encryption and hashing function schemes.

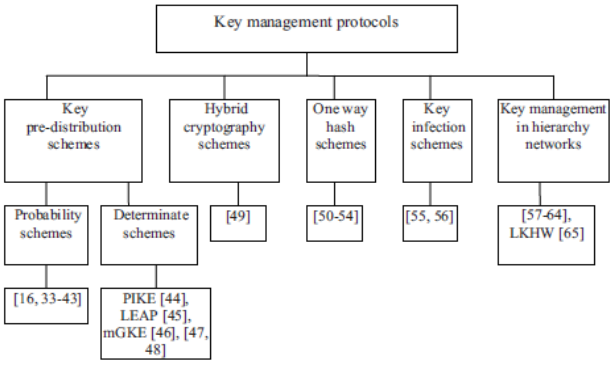

Fig 2 Taxanomy of key management protocol

They did a series performance evaluation experiments for these choosing algorithms based on different hardware platforms including Atmega 103, Atmega 128, M16C/10, SA- 110, PXA250 and UltraSparc2[8][7]. Experimental measurements indicate uniform cryptographic cost for each encryption class and each architecture class and negligible impact of caches. RC4 is shown to outperform RC5 for the Motes Atmega platform contrary to the choice of RC5 for the Motes project, a choice driven in large by memory constraints. From the findings and the experimental data, they derived a model that allows the interpolation of performance for other architectures.Their model assesses the impact of arbitrary embedded architectures as a multi-variant function for each encryption scheme depending on processor frequency, word width, ISA type and specific ISA support.

2) Cryptography Architectures*:* Some researchers implement cryptography with software in normal sensor networks' hardware. For example, Malan, propose the first known implementation of elliptic curve cryptography for sensor networks based on the 8-bit, 7.3828-MHz MICA2 mote. Others implement cryptography with specific cryptography design in hardware. Some approaches are based on symmetric cryptography, while others use asymmetric cryptography or both. Most asymmetric cryptography architecture balance the overheads between sensors and base stations. Some approaches adopt both asymmetric and symmetric cryptography to ease the overheads. For example, a security architecture proposed by Schmidt, includes three different interacting phases: a pairwise key agreement to provide authentication and the initial key exchange, the establishment of sending clusters to extend pairwise communication to broadcast inside the communication range, and encrypted and authenticated communication of sensor data.

IV. SUMMARY

Security in sensor networks is a new area of research, witha limited, but rapidly growing set of research results. Becauseof 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[7].

• 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 keypredistribution; 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 ad hoc 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; etc.

• 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.

REFERENCES

[1] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in Proc. International Conf. Mobile Computing Networking, 1999, pp. 263–270.
[2] J. W. Gardner, V. Varadan, and O. Awadelkarim, Microsensors, MEMS and Smart Devices. New York: Wiley, 2001.
[3] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for network sensors," in Proc. ASPLOS-IX, 2000.
[4] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile networking for "smart dust," in Proc. International Conf. Mobile Computing Networking, 1999, pp. 271–278.
[5] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, pp. 102–114, 2002.
[6] E. Shi and A. Perrig, "Designing secure sensor networks," IEEE Commun. Mag., vol. 11, pp. 38–43, 2004.
[7] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," IEEE Commun. Surveys Tutorials, vol. 7, pp. 2–28, 2005.
[8] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, 2006.

