Security in Mobile Wireless Sensor Networks

Kashif Kifayat, Madjid Merabti, Qi Shi, David Llewellyn-Jones
School of Computing & Mathematical Sciences, Liverpool John Moores University, UK
K.Kifayat@2004.ljmu.ac.uk, {M.Merabti, Q.Shi, D.Llewellyn-Jones}@ljmu.ac.uk

***Abstract*— Security in wireless sensor networks has become a primary concern in order to provide secure communication between static and mobile sensor nodes. As interest in wireless sensor networks continue to grow, so does the need for effective security mechanisms. Because sensor networks may interact with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design. Unlike traditional networks, the unique characteristics of mobile sensor networks pose a number of nontrivial challenges in security design, such as open peer-to-peer network architectures, shared wireless medium, stringent resource constraints and highly dynamic topology. In this paper we survey the major topics in mobile wireless sensor network security, and present the obstacles to and the requirements for mobile sensor security. Finally we propose a security model for mobile wireless sensor networks.**

I. INTRODUCTION

Humans always invent new technologies according to their needs. Wireless Sensor Networks (WSNs) are newly developed sensor networks consisting of multifunctional sensor nodes that are small in size and communicate undeterred over short distances. Sensor Networks provide more and unique facilities to users, which were not possible in the past. Sensor nodes incorporate properties for sensing the environment, data processing, and communication with other sensors. A WSN has a wide range of applications including patient health monitoring, environmental observation and building intrusion surveillance. However along with unique and different facilities WSNs have different and uniquely challenging issues (*e.g.* limited resources) compared to traditional networks. In particular, nodes are battery operated, often having limited energy and bandwidth available for communications. With such restricted resources, providing better security is a challenge.

Secure communication between network components is always an issue and researchers are continually inventing new security protocols to provide increasingly secure communications. WSNs have the same security challenges as traditional networks but with the additional challenge of the limited recourses of sensor nodes. As a result, we are unable to use traditional techniques for WSNs.

Nonetheless, WSN security often assumes that nodes are static, and share the same neighbours and location throughout their lifetime. Yet new scenarios are being envisaged where this is no longer the case, and where nodes may move both logically and physically. This development of *Mobile Sensor Networks* (MSNs) alters existing assumptions and although security has long been an active research topic in traditional networks, the unique characteristics of MSNs present a new set of nontrivial challenges to security design. These challenges include open network architectures, shared wireless medium, resource constraints, scalability, and highly dynamic network topology. Consequently, the existing security solutions for traditional networks, mobile ad hoc networks and static sensor networks do not directly apply to Wireless and Mobile Sensor Networks.

The ultimate goal of the security solutions for MSNs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile nodes. In order to achieve this goal, any security solution should provide complete protection spanning the entire protocol stack [3].

Due to the different characteristics and puerile age of MSNs there is a lack of a clear line of defence from the security design perspective. Unlike traditional networks that have dedicated routers, each mobile sensor node in an MSN may function as a manager, aggregator, router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers.

Due to the absence of a clear line of defence, a complete security solution for MSNs should integrate and encompass all three components: *prevention*, *detection*, and *reaction*. For example, the prevention approach can be used to ensure the correctness of routing states and to establish secure communication between sensor nodes, while the detection approach can detect any malicious activities. Finally the reactive approach can be used

ISBN: 1-9025-6016-7

to cure any security damage or security flaws. As argued in Zhang and Lee [4], security is a chain, and it is only as secure as the weakest link. Missing a single component may significantly degrade the strength of the overall security solution.

As describe in Yang *et al.* [3], security never comes for free. When more security features are introduce into the network, in parallel with the enhanced security strength is the ever increasing computation, communication, and management overhead. Consequently, network performance, in terms of scalability, service availability, robustness, and so on of the security solutions becomes an important concern in a resource-constrained MSN.

This paper aims to provide a survey on Security in Mobile Sensor Networks, which highlights and consider major security issues and implications of MSNs in more depth. The remainder of the paper is organized as follows: In the next section we consider the different types of MSN. We then go on in Section III to consider their security implications, characterising them in terms of whether they fall under *prevention*, *detection* or *reaction* components. In Section IV we consider attack types, followed in Section V by a consideration of the specific challenges that MSN security architecture must overcome. This leads us to discussion of an integrated security solution in Section VI, after which we present future work and conclude in Section VII.

II. Mobility in Wireless Sensor Networks

In a mobile sensor network we need to assume certain parameters (e.g. network type, application model and node roaming type) before proposing any security scheme. Network type covers various possibilities, for example a mobile sensor network can be the combination of mobile and static sensor nodes, or it may contain all mobile sensor nodes. Furthermore we also need to specify the application model and sensor node roaming type.

A. Application Models

A mobile sensor network can apply to different applications. We describe two different application models for mobile wireless sensor networks. The first model is a geographical partition model. The entire area is divided into several adjacent regions, with a different group in each region. This model can be used to model a battlefield situation, where different battalions are carrying out similar operations (e.g. land mine searches) in different areas. Each group is in charge of one partition.

The second model is a ‘convention’ scenario. It models the interaction between exhibitors and attendees. In a convention, several groups give demos of their research projects/products in separate but connecting rooms. A group of attendees roams from room to room. They may stop in one room for a while and then move on to another room. Or, they may pass through one room quickly. This is called the Convention Model [9].

B. Types of Roaming

We assume two types of mobile sensor node roaming: free roaming and guided roaming. In free roaming mobile sensors can freely roam without any restriction e.g. a sensor network located in the sea. In guided roaming the movement of the mobile sensor nodes is pre-planned either by a group leader or the sink according to operation e.g. battle field, traffic monitoring etc. Security should be considered for all possible types of mobile sensor networks.

III. Security Systems for Mobile Sensor Networks

In this section we present different security paradigms, organised into two different parts: low level security and high level security. As discussed earlier, a complete security solution for MSNs should integrate and encompass all three components: prevention, detection, and reaction. We need to identify the position of every paradigm in these three components (prevention, detection, and reaction).

A. Low level security in MSNs

We will consider various low level security properties individually.

1) Authentication: Authentication is important for mobile sensor networks to enable static and mobile sensor nodes to notice maliciously injected or spoofs packets. This is particularly important since sensor networks use a shared wireless communication medium. However authentication does not solve the problem of compromised nodes. As a compromised node has the secret keys of a legitimate node, it can authenticate itself to the network. Nevertheless to identify compromised nodes we may be able to use intrusion detection techniques [7].

To establish efficient authentication in mobile sensor network is more challenging problem then in static sensor networks. In a static sensor network every sensor node might have fixed number of neighbours, and new sensor nodes are unlikely to be added after deployment. However in a mobile sensor network nodes easily roam from one place

to another. To provide authentication in large scale mobile sensor networks is a challenging task due to the limited resources of every sensor node. *Authentication provides better security at prevention level.*

2) Secrecy: In order to secure data from eavesdroppers, ensuring the secrecy of sensed data is necessary.

In mobile sensor networks data secrecy might have a higher risk level then in static sensor nodes due to their roaming and the sharing of information with other sensor nodes. Therefore mobile sensors should not leak sensor readings to neighbouring nodes without proper security. We recommend that keys used for data encryption are not shared with neighbouring nodes *to provide secrecy is also the responsibility of the prevention component.*

To provide secrecy we can use standard encryption functions and a shared secret key between the communicating parties. To protect the privacy of data, encryption itself is not sufficient as an eavesdropper can perform traffic analysis on the overheard cipher text and this can release sensitive information about the data. Furthermore, to avoid misuse of information, privacy of sensed data also needs to be enforced via access control policies at the base station [7].

3) Availability: Providing availability requires that the mobile sensor network should be functional throughout its lifetime. Denial of Service (DoS) strikes usually result in failure of availability or may allow node capture attacks. Loss of availability may have serious impacts. In some application e.g. manufacturing monitoring applications, loss of availability may cause failure to detect a potential accident and that results in financial loss; loss of availability may also open a back door for enemy invasion in battlefield surveillance applications [7]. *The availability falls under the responsibility of detection and reaction components.*

4) Key Establishment and Management: In wireless sensor network applications, communications can be monitored and nodes are potentially subject to capture and surreptitious use by an adversary [1]. For this reason cryptographically protected communications are required. A keying relationship can be used to facilitate cryptographic techniques. To make a secret and authenticated link for two sensor nodes, it is important to create a shared secret key.

There are two simple strategies for key management schemes. One is to use a single secret key over the entire network. This scheme is obviously efficient in terms of the cost but compromise of a single node exposes all communications over the entire network, which is a serious deficiency. The other extreme is to use distinct keys for all possible pairs of nodes. A typical scheme to fulfil this is to preload every node with $n - 1$ keys, where n is the network size. This scheme guarantees perfect resilience in that links between non-compromised nodes are secure against any coalition of compromised nodes. However this scheme is not suitable for large networks since the key storage required per node increases linearly with the network size [2]. Due to the need for secure communication and with only limited resources, researchers are proposing solutions that fall between these two strategies.

For key establishment a popular method is the use of public key cryptography, but for many applications the computational cost of this is likely to be too high. Researchers have proposed many key management solutions for static sensor networks [10]. However further research is necessary for mobile sensor networks in order to improve these algorithm in terms of resilience to node compromise, scalability, memory requirement and communication overhead [7]. *Key management perfectly fits into the prevention component of an integrated secure model for mobile sensor networks.*

5) Privacy: Sensor networks have thrust privacy unease to the forefront. One of the risks is that ubiquitous sensor technology might permit ill intentioned individuals to deploy secret surveillance networks for spying on unaware victims. Technology trends suggest that as time passes the problem will get worse. *Privacy also falls under the responsibility of the prevention component.*

The networked nature of mobile sensor networks elicits new fears which are qualitatively different from those private citizens faced before. Sensor networks permit data collection, coordinated analysis and automated event correlation [6].

6) Robustness to communication denial of service: A Denial of service attack is an adversary's attempt to disrupt operation and eliminate a network's capacity to perform its expected function by broadcasting a high energy signal. The entire communication systems could be jammed if the transmission is strong enough. Some other attacks are also possible like inhibiting communication by violating the MAC protocol.

One of the standard protections against jamming is the utilization of spread spectrum communication. However, cryptographically secure spread spectrum radios are not available commercially. Also, this protection is not secure against adversaries who can capture nodes and remove their cryptographic keys [6].

Each network layer in a sensor networks is vulnerable to different DoS attacks and each layer has different options available for its defence. Some of the attacks crosscut multiple layers or exploit interactions between them. *This type of security service should be provided the by detection and reaction components.*

7) Secure Routing: The main challenge is to ensure that each intermediate node cannot remove existing nodes or add extra nodes to the route. In the real world, a secure routing protocol guarantees the integrity, authenticity and availability of messages in the existence of adversaries of arbitrary power. Every authorized receiver should receive all messages that proposed for it and would be capable to prove the integrity of every message and also the identity of the sender [5]. Secure routing can be challenging task in mobile sensor network due to frequent change in topology as compare to static sensor nodes.

Attacks on sensor network routing are possible because most sensor networks routing protocols are quite simple, and for this reason they are sometimes susceptible to attacks. According to Karlof C. et al. "Most network layer attacks against sensor networks fall into the following categories.

- *Spoofed, altered, or replayed routing information*
- *Selective forwarding*
- *Sinkhole attacks*
- *Sybil attacks*
- *Wormholes*
- *HELLO flood attacks*
- *Acknowledgement spoofing*."

By *spoofing*, *altering*, or *replaying* routing information, an adversary might be capable of creating routing loops, attracting or repelling network traffic, widening or shortening source routes or creating bogus error messages etc. [5].

In *Selective Forwarding Attacks*, malicious nodes can refuse to forward certain messages and simply drop them. Such a malicious node behaves like a black hole, swallowing every packet it's supposed to forward [5]. These nodes can be mobile or static.

The *Sybil Attack* is one of the most dangerous attacks against sensor and ad hoc networks. In this attack the malicious node behaves as if it were a larger number of nodes. In this type of attack that particular node represents various identities to other nodes in the network. This attack can decrease significantly the effectiveness of fault tolerant schemes such as distributed storage, dispersity, multipath routing and topology maintenance. *Secure routing should be the responsibility of all three components.*

8) Resilience to node capture: One of the tough issues facing sensor networks is resilience against node capture attacks, where an adversary gains full control over a sensor node through direct physical access. It is usually assumed that node capture is easy. A node capture attack can be fatal when sensor nodes share keys with neighbouring nodes used for encryption and can lead to the compromise of communication across the entire sensor network. The attack can be even more effective in mobile sensor networks if mobile nodes are being compromised. *To handle such a fatal attack all three components, prevention detection and reaction need to work together.*

In a traditional computer network it is generally assumed that hackers can be denied physical access to our computers. But sensor networks upset that paradigm. The possibility exists for a hacker to capture sensor nodes, extract cryptographic secrets, change a node's programming or replace it with a malicious node under the attacker's control. One of the protections might be the use of tamper resistant packaging, but this is costly and current technology does not offer a high level of security. Therefore, algorithmic solutions to the problem of node capture are preferred [6].

B. High level security in MSNs

1) Secure Group Management: Usually in large scale networks researchers spilt the entire network into small groups of nodes for efficient communication. Consequently large scale wireless sensor networks can be managed in groups. However secure protocols for group management are required for this.

Secure group management can be more challenging in MSNs then in static sensor networks, since in an MSN there can be frequent movement (joining and leaving) of nodes between groups, which can create more vulnerabilities, especially when malicious mobile nodes exist in

the MSN. *Secure group management can be provided with help from the prevention, detection and reaction components.*

2) Intrusion Detection: Wireless sensor networks are susceptible to many forms of intrusion. At various concentration points in wired networks, traffic and computation are typically monitored. But in terms of memory and energy consumption this is costly, so wireless sensor networks need a fully distributed solution that is cheaper in terms of energy, computation and memory requirement [6].

Intrusion prevention techniques such as encryption and authentication can be used in ad hoc networks to reduced intrusion but it cannot eliminate it [4]. *This type of security service should be provided by the detection component.*

3) Secure Data Aggregation: One benefit of a wireless sensor network is the fine-grained sensing that large and dense sets of nodes can provide. The sensed values must be aggregated to avoid overwhelming amounts of traffic being sent back to the base station. For example, the system may average the temperature or humidity of a geographic region, combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection. Depending on the architecture of the wireless sensor network, aggregation may take place at many places in the network. All aggregation locations must be secured [6] and the aggregator node can be mobile. *This type of security service should be provided by the prevention component.*

IV. ATTACKS

A. Passive Attacks

In a passive attack, the attacker node is not an authorized participant of the sensor network. As the sensor network communicates over a wireless channel, a passive attacker can easily eavesdrop on the network's radio frequency range, in an attempt to steal private or sensitive information. Interception of sensitive information might contain the physical location of a sensor node allowing an attacker to locate the nodes and destroy them, or application specific content etc.

The adversary could also alter or spoof packets, to break the authenticity of communication or inject interfering wireless signals to jam the network [7].

B. Active Attacks

Node compromise is the central problem that uniquely characterizes the sensor network threat model. With node compromise, an adversary can perform an insider attack. In contrast to disabled nodes, compromised nodes actively seek to disrupt or paralyze the network. A compromised node may exist in the form of an enemy sensor node (e.g. a captured sensor node that has been reprogrammed by the attacker); or it can be a more powerful device such as a laptop, with more computational and memory resources and a more powerful radio. A compromised node has the following properties.

- The device is running some malicious code that is different from the code running on a legitimate node and seeks to steal secrets from the sensor network or disrupt its normal functioning.
- The device has a radio compatible with the legitimate sensor nodes such that it can communicate with the sensor network.
- The device is an authorized participant in the sensor network. Assuming that communication is encrypted and authenticated through cryptographic primitives, the device must be in possession of the secret keys of a legitimate node such that it can participate in the secret and authenticated communications of the network. In the worst case, a compromised node can exhibit arbitrary behaviour, which is well known as the Byzantine model [7, 8].

V. CHALLENGES

The nodes' mobility poses far more dynamics in MSNs compared to Static Sensor Networks (SSNs). The network topology is highly dynamic as nodes frequently join or leave the network, and roam throughout the network. The wireless channel is also subject to greater interferences and errors, revealing volatile characteristics in terms of bandwidth and delay. With such dynamics, mobile nodes may request for anytime, anywhere security services as they move from one place to another.

Security research into WSNs is still in its early stages. Existing proposals are typically attack-oriented in that they first identify several security threats and then enhance an existing protocol or propose a new protocol to ruin such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. For example key management cannot provide full resilience against node capture attacks.

Therefore we need integrated security solutions that can be embedded into every possible component in the network, providing in-depth protection that offers multiple lines of defence against many – both known and unknown – security threats. We need to take all possible threats and parameters into account that affect security.

VI. Integrated Security Solution

Due to the absence of a clear line of defence, a complete security solution for MSNs should integrate all three components: *prevention*, *detection*, and *reaction*. The prevention component prevents the attacker by increasing the complexity of penetrating the system. However, the history of security has clearly shown that a completely intrusion-free system is infeasible, no matter how carefully the prevention mechanisms are designed. This is especially true in MSNs, consisting of mobile sensor nodes that are prone to compromise or physical capture. Therefore, the detection and reaction components that discover the rare intrusions and take reactions to avoid persistent adverse effects are crucial for the security solutions to operate in the presence of limited intrusions [3].

In the MSN context, the prevention component is mainly achieved through key management and routing protocols that prevent the attacker from installing incorrect routing states at other nodes. The detection component discovers ongoing attacks. Such attacks can be detected either by end-to-end methods or by neighbouring nodes. Once the attacker node is detected, the reaction component makes adjustments to exclude such a node.

VII. Conclusion

In this paper, we introduced mobile sensor networks, their related security problems and presented the major parameters affecting security. In mobile sensor networks dynamic change of topology, scalability and limited recourses are all major issues making security a tough challenge for researchers.

Existing proposed solutions are specific to static sensor network solutions and designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore we need to use a complete security package for mobile sensor networks. This package must contain three integrated components: *prevention*, *detection*, and *reaction*. The prevention model will prevent attacker from launching attacks, the detection model will detect malicious nodes and finally the reaction model will take possible countermeasures to cure the problem.

In our future work we intend to adopt same three tier security model to provide better security for Mobile Sensor Networks.

References

[1] L. Eschenauer and V. Gligor, “A Key Management Scheme for Distributed Sensor Networks” , CCS 2002

[2] J.Leeand and D.R.Stinson. Deterministic key predistribution schemes for distributed sensornetworks. Lecture Notes in Computer Science 3357 (2005), 294-307

[3] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and solutions" (2004). IEEE Wireless Communications. 11 (1), pp. 38-47.

[4] Y. Zhang, W. Lee, “Intrusion detection in wireless ad-hoc networks”, ACM MobiCom, 2000

[5] Karlof, C. and Wagner, D. “Secure routing in wireless sensor networks: Attacks and countermeasures”, In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (Anchorage, AK, May 11, 2003).

[6] Adrian Perrig, David Wagner and Jack Stankovic, “Security in Wireless Sensor Networks”, In Communications of the ACM, 47(6), June 2004.

[7] Shi E, Perrig A (2004), “Designing Secure Sensor Networks”, Carnegie Mellon University, Appears in Wireless Communication Magazine, 11(6), December 2004.

[8] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem,” ACM Trans. Programming Languages and Systems, vol. 4, no. 3, July 1982, pp. 382–401.

[9] Gerla, M.; Kaixin Xu; Xiaoyan Hong, “Exploiting mobility in large scale ad hoc wireless networks”, CCW 2003, pp. 34 – 39

[10] Kashif Kifayat, Madjid Merabti, Qi Shi, David Llewellyn-Jones, “Application Independent Dynamic Group-Based Key Establishment for Large-scale Wireless Sensor Networks”, China Communication Journal, Special issue on Communication and Information Security in Feb, 2007