WIRELESS SENSOR NETWORK SECURITY

S. Jagadeesan

Dept. of CSE, SRM University (India)

ABSTRACT

Wireless Sensor Network (WSN) is an talented skill that shows huge secure for various Applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it plenty in future. The addition of wireless communication technology has various types of security threats. The security related issues and challenges in wireless sensor networks identify the security threats, review proposed security mechanisms for wireless sensor networks. These networks are likely composed of hundreds and potentially functioning separately in many cases without access to renewable energy resources. The need for invisible deployments will result in small sized, resource-constrained sensor nodes. The set of challenges in sensor networks are varied and focus on security of Wireless Sensor Network. To proposed the security goal for Wireless Sensor Network security being crucial to the acceptance and use of sensor networks for many application and in depth threat analysis of Wireless Sensor Network.

Keywords: WSN, Security Issues, Types of Attacks, Sensor Technology

I. INTRODUCTION

The wireless sensor network becomes more and more frequent especially in data sensitive environment. Many sensor networks contain proposed wireless sensor network routing protocols with security goals. The uses of wireless sensor networks most recent semester and our research alert on their use in Mass Causality Events (MCE). In these events motes are attached to a patient's wrist and are tasked with transmitting essential information about the patient's condition, medical history and personal data to urgent situation human resources. The transmitting of private data over wireless communication became an obvious security concern and was identified as one of the primary challenges to the use of wireless sensor networks. So the security topics encouraged us to reexamine current security measures in place and explore new security concerns and how they are being approached. Many protocols are currently unconfident and can become secure simply by incorporating existing security mechanisms into their design. With the assertion that wireless sensor network protocols must be proposed with security as a priority to achieve secure routing. This document presents the background of the existing problem in wireless sensor networks coupled with what is required for secure routing protocols. Furthermore presents various attacks and security analysis on current protocol designs as well as countermeasures and security services available to defend those attacks.

II. SECURITY CHALLENGES

The biggest challenge for securing wireless sensor networks is the lack of existing resources within these networks. Each node contains very little resources; computational power, power sources, and memory are at a premium. Power is considered the scarcest resources of all. For example, the power consumption of a node, in particular the Berkley Mica mote is three times greater when the node is required to perform an action such as listening to or transmitting data. All of the potential security measures or defenses discussed in this paper would require some re-allocation of the networks existing resources. Public-key cryptography would require so many of these resources that it is considered basically an usable defense measure. The second challenge plaguing security is the size of existing communication bandwidth. The transmitting of bits can consume significant power among the networks. Therefore, if we expand the message size to account for additional security measures, we have another severe power drain. Insider attacks, as discussed in earlier sections, are virtually impossible to prevent. In these attacks, the intruder has been previously granted all levels of basic security, such as access control, network access. If an individual with inside access becomes corrupt or decides to intrude upon the network, there is very little that can be done to prevent it. Unfortunately, wormholes and sinkholes present another challenge. These attacks are also considered unpreventable after the network has been designed, especially if they are used in combination.

III. BACKGROUND PROBLEM STATEMENT

The following describes the network setting and the assumptions and goals of a secure network protocol.

Network Assumptions

There are many assumptions that can be made about the wireless sensor network. These networks use wireless communications which are typically radio links inject much security concern into our network. Radio links are prone to intruder eavesdropping, the injection of bits into the channel and the recording and replay of previously heard packets. The second main network assumption deals with the physical aspects of the sensor nodes. An attacker can either insert malicious nodes into our network or tamper with an existing node. These new nodes are capable of colluding to attack the network. An intruder can capture critical data from a tampered node.

Trust Requirements

The key trust requirement for wireless sensor network protocols is reliability. Due to the reality that networks rely heavily on base stations as the interface to the outside world and to send dependable messages are important to be able to assume that they are trustworthy. The ability to trust them if necessary and assume they will perform correctly under the applied circumstances. If a significant number of base stations are compromised the network is deemed useless. In addition to the trustworthiness of base stations have to be concerned with the trustworthiness of aggregation points are typically regular nodes and are assumed to accurately combine messages from nodes and forward them to the base stations. The tricks to aggregation tampered nodes are capable of colluding to attack the network. The ability to trust them if necessary and assume they will behave correctly under the applied circumstances. An outsider attacker does not have authorized access to the network or its nodes. An insider attack, therefore, is just the opposite. In this form of attack, the attacker does have authorized access but has "turned bad." Insider attacks can occur by either compromised nodes running malicious code or adversaries who have stolen information from good nodes and are using a lap-top class device to attack the network.

3.1 Security Goals

Every secure routing protocol should guarantee the integrity, authenticity and availability of messages in the presence of adversaries of arbitrary powers. With this statement in mind can be identified. The first goal addressed deals with preventing eavesdropping caused by misuse or abuse of the routing protocol in place. Secrecy of the application data can be corrupted by eavesdropping however, secrecy is not typically a goal of the routing protocol. In addition, protection against the replay of valuable data packets is a security goal that cannot be achieved using the routing protocol. This goal can be obtained by the application layer.

These goals, however, are much harder to obtain when considering an insider attack. It is almost impossible to prevent against an insider attack.

3.2 Requirements for Sensor Network Security

The requirements dealing with security in a wireless sensor network can be broken down into four main categories; data confidentiality, data authentication, data integrity, and data freshness. These four categories are explained in detail by the following subsections.

Data Confidentiality: Typical wireless sensor networks are used in environments where highly confidential and sensitive data is being distributed. Sensor networks should not leak information and sensor readings to neighboring networks. An example of the need for confidentiality is the use of a wireless sensor network in an emergency medical situation. Patient information being transmitted to caregivers via nodes should maintain be kept private and confidential. The key to achieving confidentiality in these protocols is to implement encryption and symmetric key authentication. This will ensure that all data is kept secret through encryption of that data and only intended receivers possess the information and are able to decrypt it.

Data Authentication: In sensitive situations and more importantly in situations where decisions are being made based on transmitted data, authentication is pertinent. Data authentication allows a receiver to verify that the data really was sent by the claimed sender. This is important because an adversary can easily inject messages into the network. This is considered one of the most common forms of attacks. The receiver needs to be able to identify the sender and ensure that the data is valid before operating on that data. Achieving data authentication can be done with symmetric key mechanisms in two party communications. This is simply a network where the two parties share a single secret key for passing messages. Only when the correct key is transmitted do they accept messages. This does not work for broadcast settings and were multiple notes and base stations are in play. If all nodes are sharing the same secret key and you only want a single node to receive the message it is insecure. Any of the nodes who know the secret key have direct access to that data. The way to defend this is to use an asymmetric key authentication. Nodes construct an authenticated broadcast from symmetric key primitives and then introduce asymmetry with a delayed key disclosure and one way function key chains.

Data Integrity: Data integrity is a very important requirement for data transmission and communication. It is, however, very difficult to achieve. Data integrity ensures the receiver that the data he/she received is not altered in any way in transit by an adversary. This is very difficult to detect without authentication of the data.

Data Freshness: The reason wireless sensor networks exist to achieve communication between nodes and base stations in an efficient and timely manner. Communication of data is not efficient if it is not fresh, meaning recent and no adversary replayed old messages. There exist two types of freshness, weak-freshness and strong-freshness. Their definitions are somewhat implied, but weak-freshness provides partial message ordering, and carries no delay information, and strong freshness provides a total order and allows for delay estimation.

IV. ATTACKS ON SENSOR NETWORKS

Wireless sensor networks are very susceptible to attacks due to the nature and simplicity of their protocol design. The most network layer attacks against sensor networks fall into one of the following categories described below.

4.1 Altered Routing Information

The first of the five types of attacks is altered routing information, the most common attack on sensor networks. This attack on the routing protocol targets the routing information exchanged between two nodes and is the most direct of all five of the attacks. Intruders are able to lengthen or shorten source routes, create routing loops, repel and/or attract network traffic, or generate false error messages by altering routing information.

4.2 Selective Forwarding

An essential function of a multi-hop network is that the member nodes forward and receive messages. An intruder initiates a selective forwarding attack by inserting malicious nodes into the network. These nodes will refuse to send or will drop certain messages. This type of attack has two extremes; a node can act like a black-hole and drop every received packet or a node can selectively drop and forward packets as controlled by the intruder. The former is much more obvious and more easily be detected by both the other nodes and the network administrator. The later is much less obvious and is more effective. These mechanics of the selective forwarding attack can be tricky, potentially impossible. This technique is considered more effective when the intruder is included in the path of data flow.

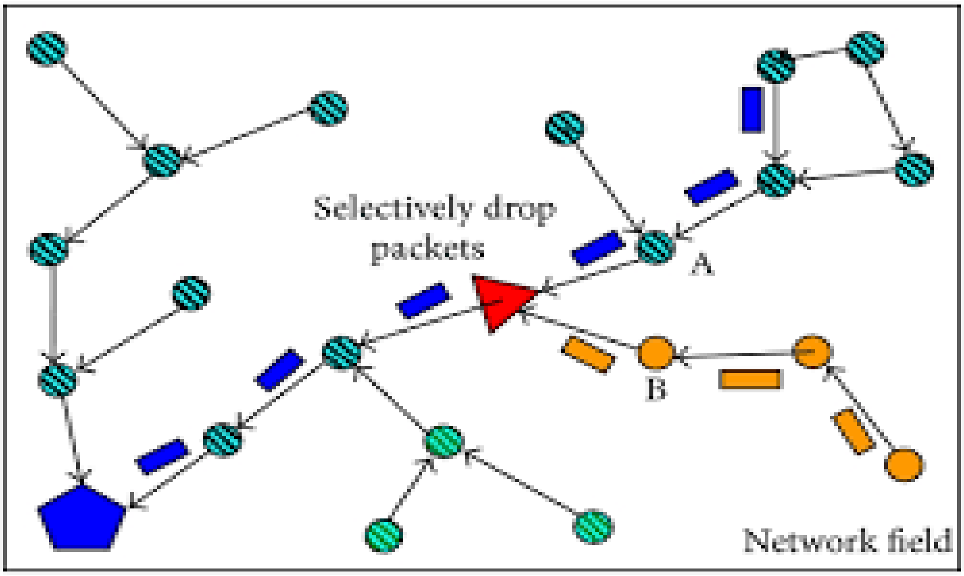

Fig 4.1 Routing Information Selectively Drop Packets

4.3 Sinkhole Attacks

Sinkholes are a multifunctional attack. Not only can they be a standalone attack but they can cause a domino effect and initiate other types of attacks as well. Sensor networks are especially susceptible to these attacks due to the configuration of their communication patterns. In a standalone sinkhole attack, adversaries try to lure nearly all the traffic from an area in the network through a centralized node which they have compromised. These attacks tend to work because the compromised node makes itself look like an attractive path through the routing algorithm. They do this by processing a high quality route and use as much power as they can to transmit the data from the node to the base station in one hop

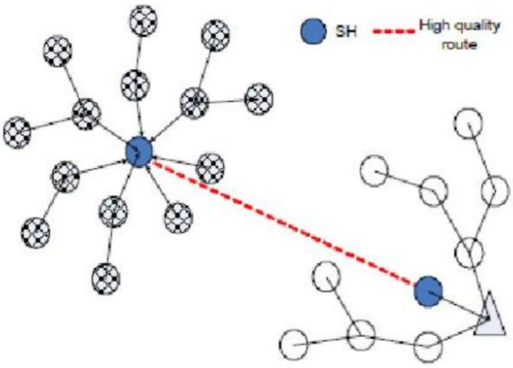

Fig 4.2 Sinkhole Attack

Thus, it is likely that all other nodes will transmit there data destined for the base station through the adversary. Mounting a sinkhole attack makes selective forwarding trivial. The compromised node, if operating accordingly, will have control of all data headed for the base station. It can then selectively suppress or modify packets that came from any node in the area.

4.4 The Sybil Attack

The Sybil attack is very straightforward. An adversary node inserted into the network simply presents multiple identities to the network. By doing so, it greatly reduces the effectiveness of the network in terms of fault-tolerance, routing, and maintenance. The Sybil attack is most effective in geographic routing protocols. Such protocols often process communication between nodes by passing a pair of coordinates to their neighbors. Essentially, with the Sybil attack a node adversary can "be in more than one place at once.

4.5 Wormholes

The underlying purpose of a wormhole is to replay messages in a network. An adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. Packets transmitted via the wormhole have a lower latency than those traveling between those same nodes over the normal network. Wormholes have a conniving way about them. They have the ability to convince those nodes located multi-hops away from a base station that they are only a single hop away if they go through the wormhole. Again, this can cause a domino effect of attacks. If there is a sinkhole on the other side of the wormhole, nodes will send packets directly through the wormhole to the sinkhole for the most direct one hop route to the base station.

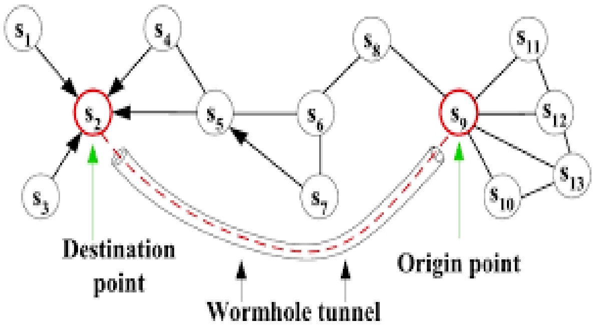

Fig 4.3 Wormhole Attack

V. SECURITY SERVICES

As we know, many wireless sensor network protocols are extremely susceptible to the above attacks, especially since much lack a proposed security goal. Below are many security services available as defenses to the above attacks on wireless sensor networks.

5.1 Outsider Attacks and Link Layer Security

As previously discussed, attacks are classified as outsider and insider attacks. Many outsider attacks can be prevented simply by implementing link layer encryption and authentication. By default many of the other types of attacks are also prevented. The Sybil attack is now impossible because nodes will not accept any of the identities locate by the adversary. Also, selective forwarding is now nearly impossible since adversary nodes are denied and cannot join the node topology. However, many insider attacks are still possible. Although new nodes are denied from joining the topology nothing prevents a wormhole from tunneling packets sent by trusted nodes to other trusted nodes. Additional defenses for insider attacks and compromised nodes are discussed in the following sections.

5.2 The Sybil Attack

Currently, there is no way to completely prevent the Sybil attack; an insider cannot be prevented from participating in the network. The best known way to defend such attacks is identity verification. Traditionally, identity verification would be done using public key cryptography, but the generation and verification of digital signatures is beyond the capabilities of sensor nodes. The suggested solution of identity verification is to have every node share a unique symmetric key with a trusted base station. Any two nodes attempting to communicate will then verify each other's identity. This raises another issue. In order to prevent an insider from making shared connections with every node, you would also have to limit the number of neighbors every node is allowed. Now, when a node is attacked and tries to communicate within the network, it can only communicate with its verified neighbors and not the entire network. Remember, that the Sybil attack can also cause a wormhole and convince two nodes that they are neighbors even if they are not. In the following section, it describes the lack of defense against wormholes.

5.3 Wormholes and Sinkholes

Wormholes and sinkholes are very difficult to defend especially when they are used in conjunction with each other. Wormholes are difficult because they use a low latency link that is hard to detect and invisible to the sensor network. Sinkholes are difficult because information they transmit is very hard for a defender to verify. It is likely that there is no effective countermeasure against these attacks that can be applied post design. The greatest defense is to build routing protocols in which these attacks are meaningless and ineffective.

5.4 Selective Forwarding

Selective forwarding is an attack that is difficult to defend due to the ease of nodes being compromised along a data flow path or placed near a base station. The best suggested defense is multi-path routing. In order to use multi-path routing the design must have completely disjoint paths, which is difficult to create. This allows for nodes to choose a packets next hop from a set of candidate nodes, reducing the adversaries' chance of gaining domination over the data flow. Messages can then be routed over many combinations of paths to reach the base station and surpass the compromised node.

5.5 Authentication Broadcasts

One of the most important requirements for a secure network protocol was for the base stations to be trustworthy. It is assumed that they are and thus the concern is that adversaries mustn't be able to spoof broadcasts of flooded messages from any of those base stations. Authenticated broadcasts are useful for localized node interactions. This would require nodes in the protocol to broadcast a HELLO message to announce themselves to their neighbors. These HELLO messages must be authenticated and spoof proof. A proposed protocol is one that uses only symmetric key cryptography and requires minimal packet overhead. It achieves the asymmetry necessary for authenticated broadcast and flooding by using delayed key disclosure and one-way key chains. Replay is thus prevented because messages authenticated with previously disclosed keys are ignored.

VI. CONCLUSION

Since we last explored the use of wireless sensor networks, little advancement has been made in making these wireless sensor networks more secure although the security need still exists. The best defenses to date are link layer encryption and authentication using a globally shared key. These mechanisms are considered to provide reasonable defense for mote-class outsider attacks which, as stated in the Challenges section, leaves the network very vulnerable to laptop-class and insider attacks. Cryptography has been explored and is basically inefficient in preventing against laptop-class and insider attacks. The resource challenge facing the networks may be one of the most difficult to overcome. The trend has shown that a factor in determining the value of a sensor network can be derived from how many sensors can be deployed. In this situation, the sensor will continue to be made as inexpensively, at the expense of resources typically, as possible to maximize the number of sensors that can be produced and deployed. In conclusion, security in wireless sensor networks remains an open issue for additional research and development. The need for these measures will only increase with widespread use and increasing popularity. Future security defenses will need to focus on using as little as possible of the sensor’s available resources, in particular its power.

REFERENCES

[1] Perrig, A., Stankovic, J., and Wagner, D. 2004. Security in wireless sensor networks. *Common. ACM* 47, 6 (Jun. 2004), 53-57.

[2] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., and Culler, D. E. 2002. SPINS: security protocols for sensor networks. *Wirel. Netw.* 8, 5 (Sep. 2002), 521-534.

[3] Hu, Y.-C., Perrig, A., and Johnson, D. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In Proceedings of IEEE Infocom 2003 (San Francisco, Apr. 1--3, 2003).

[4] L. Zhou and Z. Haas, “Securing ad hoc networks,” *IEEE Network Magazine*, vol. 13, no. 6, November/December 1999.

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Wormhole detection in wireless ad hoc networks,” Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.