Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 21 Issue 9, September 2019

A REVIEW OF SECURITY IN WIRELESS SENSOR NETWORKS

Dr. P. Karthikeyan
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: karthikeyan@jainuniversity.ac.in

Abstract

Wireless sensor networks (WSNs) can be defined as self-configured and infrastructure-free wireless networks to track physical or environmental conditions, such as temperature, sound, vibration, strain, motion or pollutants, and to transmit their data to a main location or sink where the data can be observed and processed in a cooperative manner across the network. A sink or base station serves as an interface between the network and users. By inserting queries and collecting responses from the drain, one can obtain the necessary data from the network. It is becoming important that this information be secured because of the sensitive nature of the data obtained by many wireless sensor networks (WSNs). However, conventional wireless networking security technologies are not feasible because of the finite nature of the tools available on sensor nodes due to their computing needs, power usage, speed and overhead communications. We assess the risks and attacks posed by WSNs and then review and evaluate the existing state of the art of dedicated WSN security protocols, reflecting on their respective strengths and shortcomings.

Keywords: *Denial Of Service (DOS), Eavesdropping, Injection, Interruption, Modification, Traffic Analysis*

I. INTRODUCTION

Three features will preferably include a total monitoring solution for wireless sensor networks; proactive, detective and reactive steps. Preventative strategies deter attacks, as the name implies, or at least make attacks somewhat more difficult. This is the most extensively studied field which offers authentication, integrity and secrecy using fairly common cryptographic primitives [1]. When an attack is under way in WSNs, it is always very difficult to detect and it is not easy to differentiate between an attack and a network malfunction, which is why detective steps are needed. In order to allow reactive action to be taken, it is crucial that the network, be it the nodes themselves, the base station or the end user, should differentiate between these two possibilities. The use of these reactive steps when not necessary significantly restricts the network's usefulness.

In a variety of ways, reactive steps come in. Firstly, by sending an order to each node on the network (correctly authenticated, of course), it can be as easy as shutting down the network, telling them to disable all contact for a period of time and to ignore all communication for the same period [2]. This makes it much more difficult for the attacker to operate while maintaining the energy capacity of the nodes, in the expectation that the attacker can finally go away and regular operation will be restored. Another easy choice is to allow the network to operate as usual, giving the attacker no clue of identification before the attacker is dealt with, but to ignore all transmissions [3]. These two tactics provide resilience, since after the attack subsides, the network can recover, but a committed, patient attacker can disable the network for as long as possible. More nuanced reactive steps include adjusting the level of security when an attack is underway, suppressing only infiltrated parts of a network, neutralizing attacks or even counterattacking [4]. It is complicated by computational, memory and energy resource limits to enforce these steps on wireless sensor nodes. As a result, WSN security is a trade-off between what is needed, what is ideal, and what is practicable in a practical way. The last significant obstacle in obtaining WSNs comes from the fact that they are unattended. This allows the attacker a very free rein to carry out certain attacks that in some other form of network are not feasible. This includes physical attacks, attacks on replication of nodes and attacks on the remote management interface that is also required.

Threats:

Wireless sensor networks are more vulnerable than conventional wireless networks to malware attacks. Based on the capabilities of the attacker, the extent of control by the attacker and the level of interference by the attacker, challenges to WSNs can be categorized in a variety of ways. Firstly, machines with the same functionality as the sensor nodes on the network can be used by an attacker, either by adding sensor nodes to the network distribution area or by subverting any of the nodes under attack on the network [5]. With this strategy, the spectrum of attacks is restricted since the attacker only has the same resources, particularly in terms of energy and processing capacity, as the nodes under attack. The option is that the intruder uses a personal computer/laptop fitted with the required radio, or perhaps an even more powerful dedicated unit, which would possibly communicate at a far higher power level than the radios on the sensor motors [6]. Because of the much larger energy supply, computing capacity, memory and much lower contact delay, this alternative opens up even more avenues of attack.

The primary challenge when attempting to protect a sensor network is protecting against this form of intruder. Attacks can also be categorized as attacks by outsiders or insiders. An attacker would not become a part of the network in an outsider attack. An external intruder may opt to actively listen to the contact on the network, which is very difficult to identify. However, the only protection required against this form of attack is typically the use of a sufficiently powerful cypher to protect confidentiality. The contact medium may also be directly manipulated by an external intruder. This may be achieved by interrupting (i.e. jamming) network packets or changing them, or by inserting fake packets into the network. Techniques for authentication, integrity and replay protection will detect and stop packet alteration and injection [7]. While often easy to catch, interruption attacks are difficult to protect against, particularly when dealing with an intruder from the PC/laptop class. An insider attack entails malicious code being executed on nodes that are legitimate network users. In this case, at least certain valid hidden cryptographic keys used on the network are always available by the attacker. The best defense against an insider attack is to locate these malicious nodes, a very difficult problem in general, revoke the keys they know, and ignore all possible contact from those nodes.

The potential of the intruder to achieve physical access to the sensor nodes is a challenge posed by WSNs that is not faced by other ad-hoc wireless networks. Owing to the unattended and open nature of WSN deployments, this is the case. This physical access opens up a range of threats, including reprogramming malicious code sensor nodes, extracting hidden information from the nodes, such as cryptographic keys, or even simply damaging the nodes physically. The only defense against the first two attackers is to use tamper-proof hardware, but against a certain attacker, this is both very costly and usually not very successful [8]. The only defense against the physical devastation of the nodes is to enclose the nodes in strong enclosures that are immune to destruction, but this approach is typically cost-prohibitive, not to mention the impact that such situations may have on radio contact or the sensors themselves.

Attacks:

Attacks can be either noninvasive or intrusive against wireless sensor networks. In general, non-invasive attacks consist of side-channel attacks such as strength, timing or attacks dependent on frequency. There is not much documented work on side channel attacks directly targeting WSNs, but many of the issues observed with other embedded systems could be used against sensor nodes, such as timing attacks against MAC generation or encryption [9]. Invasive attacks are much more frequent and are listed in the following sections as the most critical of these.

I. Denial of Service:

Due to the presence of attackers in the PC/laptop class, wireless sensor networks are especially vulnerable to denial of service (DOS) attacks. A DOS assault on the physical layer essentially involves the continuous propagation of a signal interfering with the radio frequencies used by the sensor network. This jamming can be persistent or periodic and can be carried out by a variety of devices in the node class or by a single powerful computer. Whatever the way the jamming is achieved, with very little intervention by the perpetrator, the sensor network may be made inefficient. On the data communication layer, DOS attacks can also be carried out. In order to create collisions, one option is to breach the contact protocol, whether 802.15.4 or Zigbee or whatever, by constantly sending messages. It is possible to deplete the capacity of targeted nodes or a targeted region of a network; as such collisions will entail retransmission by the affected node. Attacking the routing protocol requires network layer DOS attacks. A DOS transport layer attack is also feasible, but is rather reliant on the protocol of the transport layer in place on the network.

II. Attacks on Information in Transit:

On knowledge in transit between nodes, the most frequent attacks against WSNs are. In transit, information is vulnerable to eavesdropping, alteration, injection, disruption, and review of traffic. As already stated, it is possible to avoid eavesdropping, modification and injection using well-established protocols of secrecy, authentication, credibility and replay protection. In WSNs, traffic analysis can theoretically be a significant challenge that helps an attacker to chart a network's routing structure, allowing very closely focused attacks to interrupt selected parts of a network with the greater impact.

III. Node Replication Attack:

A node duplication attack entails an attacker injecting a new node into a network that has been cloned from an existing node, with current sensor node hardware cloning being a comparatively easy process. This new node will function exactly like the old node or it can have some additional behavior, such as explicitly communicating interesting information to the attacker. The problem with the second scenario is apparent, but the first situation will impact the network subtly, but also quite disruptively, probably causing routing algorithms, algorithms for data aggregation or algorithms for querying to crash. When the base station is cloned, a node duplication attack is especially serious [10]. However, the base station is also in a protected position and much more efficient than the rest of the sensor nodes for certain deployments, so cloning it are much more difficult.

II. CONCLUSION

While each of the security solutions discussed here can be used to protect a WSN efficiently, there is currently no one solution that can be 'plugged-in' to an application to provide all the necessary primitives for security. The different attacks on the Bluetooth network are discussed in this article. In depth, the Bluetooth network exposed to particular threats has been demonstrated. In the end, owing to the presence of PC/laptop type attackers, we believe that wireless sensor networks are especially vulnerable to denial of service (DOS) attacks. A DOS assault on the physical layer essentially involves the continuous propagation of a signal interfering with the radio frequencies used by the sensor network. This jamming can be persistent or periodic and can be carried out by a variety of devices in the node class or by a single powerful computer.

III. REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” *Comput. Networks*, 2002, doi: 10.1016/S1389-1286(01)00302-4.

[2] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Comput. Networks*, 2008, doi: 10.1016/j.comnet.2008.04.002.

[3] W. Sensor, *WIRELESS SENSOR NETWORKS A Networking*. 2009.

[4] J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, and M. Welsh, “Wireless sensor networks for healthcare,” in *Proceedings of the IEEE*, 2010, doi: 10.1109/JPROC.2010.2065210.

[5] V. Potdar, A. Sharif, and E. Chang, “Wireless sensor networks: A survey,” in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 2009, doi: 10.1109/WAINA.2009.192.

[6] C. Y. Chong and S. P. Kumar, “Sensor networks: Evolution, opportunities, and challenges,” in *Proceedings of the IEEE*, 2003, doi: 10.1109/JPROC.2003.814918.

[7] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: Security protocols for sensor networks,” *Wirel. Networks*, 2002, doi: 10.1023/A:1016598314198.

[8] A. S. K. Pathan, H. W. Lee, and C. S. Hong, “Security in Wireless Sensor Networks:

Issues and challenges," in *8th International Conference Advanced Communication Technology, ICACT 2006 - Proceedings*, 2006, doi: 10.1109/icact.2006.206151.

[9] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*. 2004, doi: 10.1145/990680.990707.

[10] K. Sohraby, D. Minoli, and T. Znati, *Wireless Sensor Networks: Technology, Protocols, and Applications*. 2006.