INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY ASPECTS FOR WIRELESS SENSOR NETWORK

ANAND B. DESHMUKH, MISS. POOJA VINAYAK INGALKAR

1. Asst. Prof., Sipna College of engineering and tech, Amravati, Maharashtra, India, Department of computer science and Engg.

2. Sipna College of engineering and tech, Amravati, Maharashtra, India, Department of computer science and Engg.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: A wireless sensor network (WSN) is a wireless network. It consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. Wireless Sensor Networks are a new class of ad-hoc multi-hop network that have emerged over the last five years as the most promising technology candidate for fulfilling the vision of the 'embedded Internet'. These networks consist of circuits that combine local sensing, signal processing and transceiver capabilities into a package so cost-effective that thousands of the circuits can be dispersed over a region of monitoring interest. In this paper we emphasis on exploring the security issues and challenges in WSN.

Keywords: WSN, WSD, Sensor, Architecture Attacks, Challenges.

Corresponding Author: MR. ANAND B. DESHMUKH

PAPER-QR CODE

Access Online On:

www.ijpret.com

How to Cite This Article:

Anand Deshmukh, IJPRET, 2014; Volume 2 (9): 618-624

INTRODUCTION

Wireless Sensor Network (WSN) is a low-powered wireless network formed by inexpensive devices that are battery-powered with limited computing resources. Wireless Sensor Devices (WSD) that are deployed in the field to sense physical phenomena such as humidity, temperature, vibration, light, etc…WSN contains various sensor node devices in a quite huge area Smart Environments use WSNs as one of the most crucial part for information collection. Only WSNs, which are fast and quite simple in installation as well as in maintenance, will sustain in the current scenario. Because of the less power wireless communications and accessibility of micro sensors, there are miscellaneous WSN applications domains are there. But there are many different security attacks and Challenges, we have identified, for a Wireless Sensor Network implementation. The Wireless Sensor Devices to support multichip routing to send the sensor. data from one node through another to arrive at the final destination, usually a sever for data processing.

2. WSN Architecture

Architecture of a Wireless Sensor Network consists Of the network components listed below.

Sensor Nodes –Sensor Nodes are small devices which generate a computable reaction to a variation in a physical or environmental condition.

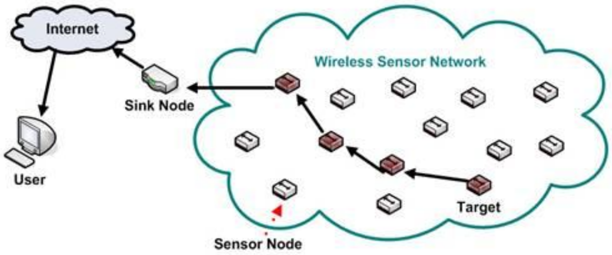

Fig: 1

These can be individually used to compute and to convert a physical or environmental amount into a signal which is read by a device or by an observer. Sensor Nodes are used for routing of packets for additional devices must be done by them only. The process or process apparatus is mostly characterized or controlled by them. There is a special type of field device, called as router, which does not have control apparatus or process sensor. Router has interface with the Process itself.

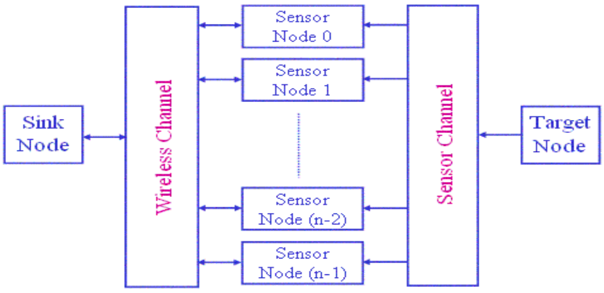

Fig: 2

3. Attacks in Wireless Sensor Network

Insider Attacks-

It is also known as Mote Class attack. In insider attacks, the attackers have unauthenticated contestant in the sensor network. These attacks are generally invoked via either corrupted sensor node running infected code or adversary who have snatched the key material, code, and data from authentic nodes, and who then uses one or more laptop class gadgets to attack the network. In this class of attack, the attacker can't access more than a few sensor nodes having same abilities to our own.

Outsider Attacks-

It is also known as Laptop Class attack. The attackers of this class have no exceptional access to the sensor network, but almost all of them can access more powerful gadgets, such as tablet PCs, notebooks etc., which replace the authentic nodes when installed for action. And these gadgets have more battery power, a sensitive antenna, a processor with better proficiencies and a stronger transmitter. The attackers might be capable of blocking the whole sensor network using its more power radio transmitter. An entire network can be collapsed just by the attack of a single attacker.

4. Challenges OF Wireless Sensor network

To protect against the attacks outlined above, system designers must be cognizant of the security properties that accompany sensor networks. Some of these properties, such as tolerable failures (Property P1) present opportunities for designing protocols for sensor networks that are infeasible in other types of networks. Below, we take a first step towards establishing a comprehensive set of security challenges for sensor networks. Some challenges are similar to those faced in more traditional environments, but with additional constraints; others are unique Sometimes one or more of these time phases may be combined. to sensor networks and similar technologies (e.g., mobile ad hoc networks [Sta02]). When steps have already been made towards a challenge, we place the related work in context.

Challenge 1: Measuring Confidentiality

Existing literature has proposed the use of computationally in expensive cryptographic techniques to handle message confidentiality and authenticity in sensor networks. The difficulty of ensuring confidentiality and authenticity is not, however, due solely to the energy constraints imposed on sensors. A sensor network is comprised of many small computing devices, each of which is subject to physical capture. Any cryptosystem must therefore tolerate the compromise of sensors and their keys. New cryptographic approaches must be developed that are geared towards this failure model. However, the compromise of some nodes need not result in a total loss of security. Unlike traditional networks in which logical information is often conveyed as single messages or packets, sensor networks rely on redundancy and aggregation (Properties P1, P2), and therefore some messages may be more influential than others. In an earlier paper [AIL05], we presented an initial

Framework for quantifying the privacy and security of sensor network applications under the assumption that some nodes may be compromised. Rather than providing all-or-nothing guarantees about privacy or security, we examined probabilistic guarantees with respect to compromise. Challenge 1 is to define models and metrics along these lines, for different protocols' logical-level information privacy and security properties.

Challenge 2: Timing Obfuscation

For a sensor value to have meaning, context is needed.

Where the value was recorded, and at what time, are necessary for interpretation. Conversely, if the time and location of one reading are known, it may be possible for

An adversary to infer a great deal about other readings nearby .Sensor networks must therefore be aware of these metadata and their role in security. It may be possible for an eavesdropper to correlate public data to infer confidential information. Deshpandeetal have proposed incorporating a probabilistic model for data aggregation in a sensor network [DGM+04]. By exploiting the correlation between different values and between different attributes, they report significant energy savings in query processing. Such a model also implies that an adversary could pose innocuous-looking queries on certain attributes to obtain confidential data. The timing of sensor messages may also reveal confidential data. we might limit the ability of an USENIX Association Hot Sec '06: 1st USENIX Workshop on Hot Topics in Security 27eavesdropper (or even the aggregating node) to infer the identity of the sensor node. Challenge 2 is to identify cost-effective schemes for hiding sensor network timing. Possible solutions might be based on sending messages at regular intervals, disassociating a reading from a physical event by adding a random delay to message transmission, or adding spurious messages to mask the legitimate send times.2

Challenge 3: Secure Aggregation

In sensor networks where aggregation occurs at intermediary nodes, end-to-end encryption from sensors to the base station is not possible because each node must be able to compute with the data. Although crypto systems have been proposed that allow computation on cipher texts [GHY87],such approaches require significant computational cost and may be infeasible in low powered devices. The standard security doctrine that the network should not be trusted and that all messages should be encrypted and decrypted at the source and destination is incompatible with aggregation (due to Property P4). Unfortunately, the alternative of trusting each link between the sensor and the base station is unappealing. Challenge 3 is to develop novel cryptographic approaches that allow the aggregation of messages while ensuring adequate security. An alternative to employing secure techniques to collect data is to use more robust statistical aggregation functions. Common aggregation functions such as average, sum, minimum/maximum are not resilient and are vulnerable to easy attacks [Wag04]. On the other hand, count, median and root mean squared error are better estimators of the data being aggregated as they are more robust.

Challenge 4: Topology Obfuscation

Unlike traditional networks, where intermediate nodes in the routing tree simply relay messages, nodes in sensor networks often carry out computation on messages before passing them along (Property P3). This computation leads to a non-uniform distribution of information across nodes: different nodes carry differing amounts of influence on the final computed value. Attacking a leaf node in a tree-structured network gains little influence (for disruption) or information (for eavesdropping); attacking a node near the root gains significant influence and information about the aggregate value (Property P1). For eavesdropping, there is an interesting third case of attacking nodes in the middle of the tree: intermediary nodes perform enough aggregation to compensate for inaccurate sensors, but their values may be local enough 2Masking timing information does not necessarily imply that aggregation cannot be performed on the data. Aggregation is performed on data that have the same logical timestamp whereas hiding the timing interferes with the ability to discern physical time. to reveal private data . Challenge 4 is to hide the routing infrastructure of the sensor network. If an adversary can attack a few chosen nodes, the obvious strategy is to compromise sensors (and their keys) that logically reside in high value locations in the routing tree.

Challenge 5: Scalable Trust Management

In the domain of sensor networks, trust management is the problem of identifying which nodes are legitimate and which are not to be trusted. The threat of physical compromise (and need to revoke trust when detected), the energy constraints, the number of nodes which must be considered, and the difficulty in re-establishing trust once sensors are deployed are all unique challenges to trust management in sensor networks. Due to the power and energy constraints of many of the nodes, it may not be possible to run expensive key generation algorithms, or to run them pair wise between every node. Even if this is feasible once, it may not be practical to run them frequently. Since there is the assumption that the physical compromise of some nodes (and therefore their shared keys) is unavoidable, limitations Must be placed on the number of nodes sharing keys to limit the impact of compromise. Key management is one of the better studied areas of sensor network security, but many of the proposed approaches are practical only under certain conditions. Challenge 5 is to develop “lightweight” key management and distribution schemes appropriate for large scale sensor networks. Due to space constraints, it is impossible to enumerate all the proposed key management systems in this paper, but the reader is referred to [WLSC].

Challenge 6: Aggregation with Privacy

The interaction between sensors and the physical world leads to new challenges in privacy and anonymity for those being sensed. Unlike traditional computing platforms, end users who are identified by sensor nodes have little ability to set policy. When browsing the Internet, for example, users can use anonym zing proxies to protect their privacy. When being sensed by a sensor, however, the end user has no input as to the level of information disclosure, and must trust in the decisions made by the sensor network. Since being sensed can be a passive act and can be done without the knowledge of the observed party, designing networks with privacy guarantees is an arduous task. Anonymity may be desired in some sensor network applications. If the objective is to be anonymous with respect to an external observer, then techniques such as Onion Routing [DMS04] could be extended to achieve anonymity. However, onion routing may be expensive 28 Hot Sec ’06: 1st USENIX Workshop on Hot Topics in Security USENIX Association here, and in some cases, it may be desirable to protect individual readings while still computing the aggregate over all readings**.** Challenge 6 is to develop new anonymity techniques to handle such requirements.

5. Conclusion

From the research papers we can conclude that The wireless sensor networks are having an extraordinary growth nowadays because of its huge number of sensor network applications in various fields. But to send and receive sensitive data within the wireless sensor networks without compromising its security is a critical job. In other words, the industry will only adopt a WSN based application, when it guarantees full security for all aspects. Although there are possibilities that upcoming research over confidentiality and authenticity in WSN will make it a

smart choice in various new fields. Recently offered security mechanisms are centered on particular network structures, hence it is less efficient to provide a complete solution for the security in wireless sensor networks. In this paper, we deeply analyzed security attacks for wireless sensor networks & proposed their preventions.

REFERENCES

1. Hiren Kumar Dev Sharma, Ajit Kumar, Sikkim Manipal Institute of Technology "Security Threats in Wireless Sensor Networks", IEEE 2006.

2. Md. Aniur Rehmam & Mitu Kumar Debnath, "Energy Efficient Data Security System for Wireless Sensor Network", Sixth International Conference on Computer and Information Technology, 2008.

3. Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Packet leashes: A Defence against Wormhole Attacks in Wireless Networks", In Proceedings of IEEE Infocom 2003, April 2003.

4. David R. Raymond, Scott F. Midriff, "Denial-of- Service in Wireless Sensor Networks: Attacks and Defenses'," IEEE Pervasive Computing, Vol. 7, No. 1, 2008, pp. 74-81.

5. Anthony D. Wood, John A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", Department of Computer Science, University of Virginia.

6. Amol Deshpande, Carlues Gustine, Samuel Madden, Joseph M. Hellrstein, and Wei Hong. Model driven data acquisition in sensor networks. In VLDB '04, 2004.