NECESSITY TO SECURE WIRELESS SENSOR NETWORK

Ms. Sonjuhi Mrinalee[1], Mr. Navin Kumar[1],Mr. Ashutosh Mishra[2], Assistant Professor[1] , Vice-Principal[2] *EC Department, Shankara Institute of Technology, Kukas Jaipur (Raj.), India*
sonjuhimrinalee@yahoo.com[1], ansunaveen.kumar@gmail.com[1,] mishra12jan@gmail.com[2]

ABSTRACT: ***Wireless sensor networks are often deployed in hostile and unattended environments. The nodes will be failure by fault, intrusion and battery exhaustion. Node-failure tolerance is an acceptable method to improve the networks lifetime. In this paper, two key problems for topology control are presented: first, how to get a node-failure topology when there is intrusion from the nodes of hostile enemies? Secondly, how to sustain this node-failure topology with all deployed nodes being exhausted ultimately? Here we suggest a novel approach for topology control and prove that it is node-failure tolerant. The approach contains three phases: topology discovery, topology update, and topology regeneration. A tricolor-based method is proposed to build architecture with high tolerance ability and some security protocols are employed to preclude the hostile nodes in discovery phase. In update and regeneration phases, the newly deployed nodes are regarded as renewable resource to fill in the consumed energy, enhance the debased node-failure tolerance ability, prolong network lifetimed. A security protocol with forward and backward secrecy is devised to adapt the topology changed by node failure and node joining. Some attributes of the presented method are shown by simulations, and differences are given by comparison with related work.***

*****

1. INTRODUCTION

One of the fundamental goals for Wireless Sensor Networks (WSNs) is to collect information from the physical world. Although there has been a number of suggestion concerning security in WSNs, provisioning security remains critical and challenging task. WSNs have attracted much attention due to its great potential to be used in various applications. Comparing to existing infrastructure – based networks,
wireless sensor networks can virtually work in any environment, especially those where wired connections are not possible. WSNs consist of battery-operated sensor devices with computing, data processing, and communicating components. The

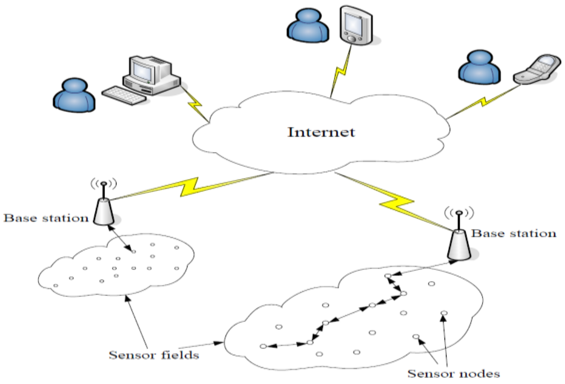


Fig.1.1 Accessing WSNs through Internet.

Ways in which the sensors are deployed can either be in a controlled environment where monitoring and surveillance are critical. In the uncontrolled environments, security for sensor networks becomes extremely important. Sensors are usually deployed in large numbers of sensor date, which are often impractical to gather from the individual sensors, particularly from the energy consummation point of view. Thus data f aggregation offers a key strategy to reduce energy consumption. Performing data fusion in WSNs can be largely attributed to two reasons- first; the user may be interested only in the aggregated results on the sensor data. Secondly, data from sensors in close proximity may be highly correlated, and data fusion can effectively reduce redundancy and hence network load. Data fusion operation has been incorporated into a wide range of existing WSN design. Although diverse work exists on data fusion, a fundamental supporting mechanism is the data routing which dictates when and where data streams will meet and hence how fusion will be performed. Apart from the wireless medium, the primary challenges for sensor networks stem from two facts. First, sensors are extremely resource constrained. Second, in many applications sensor nodes will be randomly deployed. This randomness raises the issue of dimensioning the network. Scattering too few nodes may result in lack of coverage of the sensor field and a disconnected network. On the other hand, scattering too many nodes may result in an inefficient network due to increased medium access control (MAC) collision and interference. WSNs are exploited to be deployed for a long period, and the nodes are likely to need software updates during their lifetime in order to support new requirements. In many cases the nodes will be inaccessible or too numerous to be physically accessed. This drives the need for software updates support. This paper is outlined as follows. We first introduce the general security requirements in WSNs. Then, we deal with target localization problem and security in group communications over WSNs. Finally, the importance for updating software is explained.

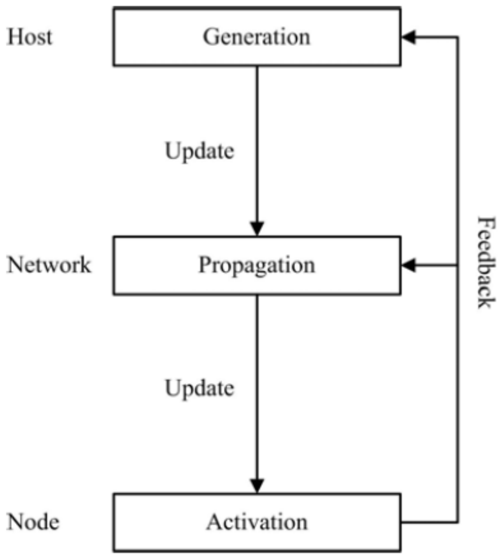


Fig. 1.2: Software update model for WSNs

2. SECURITY ISSUES

2.1 ATTACK AND ATTACKER

An attack can be defined as an attempt to gain unauthorized access to a service, a resource or information, or the attempt to compromise integrity, availability, or confidentiality of a system. Attackers, intruders or the adversaries are the originator of an attack. The weakness in a system security design, implementation, configuration or limitations that could be exploited by attackers is known as vulnerability or flaw. Any circumstance or event (such as the existence of an attacker and vulnerabilities) with the potential to adversely impact a system through a security breach is called threat and the probability that an attacker will exploit a particular vulnerability, causing harm to a system asset is known as risk.

2.2 SECURITY REQUIREMENTS

A sensor network is a special type of Ad hoc network. So it has some common property as computer network. The security requirements of a wireless sensor network can be classified as follows:

i.**Authentication**: WSN communicates sensitive data, so the receiver needs to ensure that the data used in any decision-making process originates from the correct source. Similarly, authentication is necessary during exchange of control information in the network.

ii.**Integrity**: Data in transit can be changed by the adversaries. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Data integrity is to ensure that information is not changed in transit, either due to malicious intent or by accident.

iii. **Data Confidentiality**: Applications like surveillance of information, industrial secrets and key distribution need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption.

iv.**Data Freshness:** Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To ensure that no old messages replayed a time stamp can be added to the packet.

v. **Availability:** Sensor nodes may run out of battery power due to excess computation or communication and become unavailable. It may happen that an attacker may jam communication to make sensor(s) unavailable. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the network.

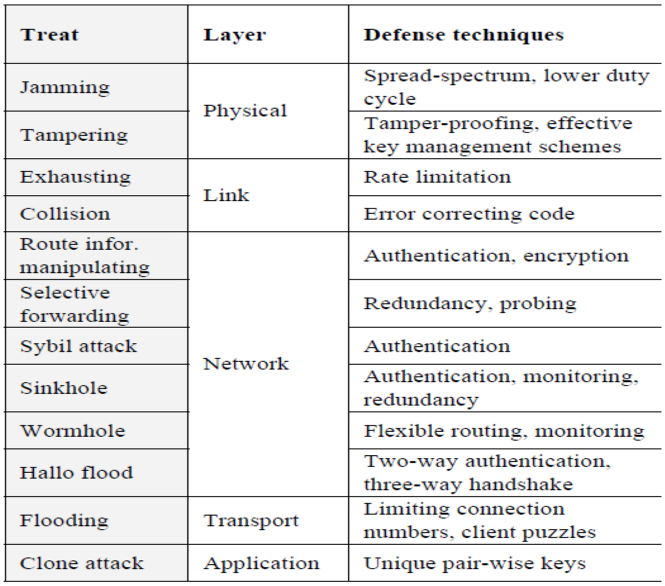
vi.**Self-Organization:** A wireless sensor network believes that every sensor node is independent and flexible enough to be self-organizing and self-healing according to different hassle environments. Due to random deployment of nodes no fixed infrastructure is available for WSN network management. Distributed sensor networks must self-organize to support multi hop routing. They must also self organize to conduct key management and building trust relation among sensors.

vii.**Time Synchronization:** Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off periodically.

viii.**Secure Localization:** The sensor network often needs location information accurately and automatically. However, an attacker can easily manipulate non-secured location information by reporting false signal strengths and replaying signals, etc.

3. THREATS TO WSN's

Communications over wireless channels are, by nature, insecure and easily susceptible to various kinds of treats. A large-scale sensor network consists of huge number of sensor nodes and may be dispersed over a wide area. Typical sensor nodes are small with limited communication and computing capabilities. These small sensor nodes are pervious to several key types of treats.



Treat	Layer	Defense techniques
Jamming	Physical	Spread-spectrum, lower duty cycle
Tampering		Tamper-proofing, effective key management schemes
Exhausting	Link	Rate limitation
Collision		Error correcting code
Route infor. manipulating	Network	Authentication, encryption
Selective forwarding		Redundancy, probing
Sybil attack		Authentication
Sinkhole		Authentication, monitoring, redundancy
Wormhole		Flexible routing, monitoring
Hallo flood		Two-way authentication, three-way handshake
Flooding	Transport	Limiting connection numbers, client puzzles
Clone attack	Application	Unique pair-wise keys

Table 3.1: Typical treats in WSNs

Treats can also be classified based on the capability of the possible attacker, such as sensor-level and laptop-level. A powerful laptop-level adversary can do much more harm to a network than a malicious sensor node, since it has much better power supply, as well as larger computation and communication capabilities than a sensor node. Treats can also be classified into outside and inside treats. An outside attacker has no access to most cryptographic materials in sensor networks, while an inside attacker may have partial key materials and the trust of other sensor nodes. Inside attacks are much harder to detect and defend against. Typical treats and adequate defense techniques in WSNs are summarized as in Table 3.1.

4. SECURITY MECHANISM

The security of wireless sensor networks has attracted a lot of attention in the recent years. Many researchers have proposed some security mechanisms. In this section, we will focus upon that mechanism, which provides better solution to the threats. In this section, we will discuss them in details.

4.1 LOCALIZED ENCRYPTION AND AUTHENTICATION PROTOCOL

LEAP provides multiple keying mechanisms that can be used for providing confidentiality and authentication in sensor networks. It supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pair wise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network. Now each of these keys is discussed and established in the LEAP protocol.

4.2 Random Key Pre distribution Schemes

Various forms of Random Key Pre distribution Schemes are:

i.**Key pre distribution phase**: A centralized key server generates a large key pool offline. The procedure for offline key distribution is that we first assign a unique node identifier or key ring identifier to each sensor. Then select *m* different keys for each sensor from the key pool to form a key ring. Load the key ring into the memory of the sensor. Sensor deployment phase: The sensors are randomly picked and uniformly distributed in a large area.

Typically, the number of neighbors of a sensor (n) is much smaller than the total number of deployed sensors (N). Key discovery phase: During the key discovery phase, each sensor broadcasts its key identifiers in clear-text or uses private share-key discovery scheme to discover the keys shared with its neighbors. By comparing the possessed keys, a sensor can build the list of reachable nodes with which share keys and then broadcast its list. Using the lists received from neighbors, a sensor can build a key graph based on the key-share relations among neighbors. Pair wise key establishment phase: If a sensor shares key(s) with a given neighbor, the shared key(s) can be used as their pair wise key(s). If a sensor does not share key(s) with a given neighbor, the sensor uses the key graph built during key discovery phase to find a key path to set up the pair wise key. The set of all neighbors of sensor i is represented by Wi. The definition of key graph is given as follows: Definition 1 (key graph). A key graph maintained by node i is defined as $Gi = (Vi , Ei)$ where, the vertices set $Vi = \{j \mid j \in Wi \vee j = i\}$, the edges set $Ei = \{ejk \mid j, k \in Wi \wedge j\ R\ k \}$, R is a relation defined between any pair of nodes j and k if they share required number of key(s) after the key discovery phase. Definition 2 (key path). A key path between node A and B

is defined as a sequence of nodes A, $N1$, $N2$,. . ., Ni, B, such that, each pair of nodes (A, $N1$), ($N1$, $N2$), . . ., (Ni-1, Ni), (Ni ,B) has required number of shared key(s) after the key discovery phase. The length of the key path is the number of pairs of nodes in it.

ii. **Purely Random Key Pre distribution (P-RKP):** There are two characteristics of current P-RKP schemes. First, the m keys preinstalled in a sensor can also be installed in other sensors. That is, a key can be shared by more than one pair of sensors. Second, in most of current schemes, there is no relation between the set of preloaded keys and the sensor ID. A recent solution proposed by Pietro et al. attempts to define this relation. However, the scheme is not scalable in that the size of the network is restricted by a function of number of preinstalled keys.

iii. **Structured Key Pool Random Key Pre distribution:** (SK-RKP) Scheme Unlike in P-RKP schemes, in SK-RKP scheme, each sensor is preloaded with a unique set of keys in its memory. The key discovery is not simply finding a shared key with the neighboring sensor, but using a set of polynomial variables (constructed by the keys possessed by the sensor) to derive the shared key. In addition, the key ID can serve as the sensor ID which is linked to the set of pre-installed keys. This link can prevent the attackers from misusing the sensors' IDs. In the following paragraphs, a brief description of structured key pool scheme is given. The SK-RKP scheme uses the key redistribution scheme proposed by Blom. This scheme allows any pair of nodes in a network to find a pair wise key in a secure way as long as no more than λ nodes are compromised. The scheme is built on two matrices: a publicly known matrix G of size $(\lambda + 1) \times N$; a secret matrix D of size $(\lambda + 1) \times (\lambda + 1)$ created by key distribution center. The matrix A of size $N \times (\lambda + 1)$ is then created as $A = (D \cdot G)\ T$. Each row of A is the keys distributed to a group member and the row number can serve as a sensor's ID. Since $K = A \cdot G$ is a symmetric matrix, nodes i and j can generate a shared key (Kij or Kji) from their redistributed secrets, where Kij is the element in K located in the ith row and jth column.

4.3 SECURITY LEVELS BASED ON DIFFERENT DATA

The mechanism for communication security in wireless sensor networks is that data items must be protected to a degree consistent with their value. There are three types of data sent through the network: mobile code, locations of sensor nodes and application specific data. Following this categorization, the three security levels described here are based on private key cryptography utilizing group keys. Since all three types of data contain more or less confidential information, the content of all messages in the network is encrypted. The mechanism is assumed that all sensor nodes in the network are allowed to access the content of any message. The deployment of security mechanisms in a sensor network creates additional overhead. Not only does latency increases due to the execution of the security related procedures, but also the consumed energy directly decreases the lifetime of the network. To minimize the security related costs, following the taxonomy of the types of data in the network, three security levels are defined:

- Security level I is reserved for mobile code, the most sensitive information sent through the network.
- Security level II is dedicated to the location information conveyed in messages.
- Security level III is applied to the application specific information.

The strength of the encryption for each of security levels corresponds to the sensitivity of the encrypted information Therefore, the encryption applied at level I is stronger than the encryption applied at level II, while the encryption on level II is stronger than the one applied at level III. Different security levels are implemented either by using various algorithms or by using the same algorithm with adjustable parameters that change its strength and corresponding computational overhead. Using one algorithm with adjustable parameters has the advantage of occupying less memory space. RC6 [12] is selected. It is suitable for modification of its security strength because it has an adjustable parameter (number of rounds) that directly affects its strength. The overhead for the RC6 encryption algorithm increases with the strength of the encryption measured by the number of rounds.

5. CONCLUSION

Security in wireless sensor networks has attracted a lot of attention in the recent years. In this paper, some security mechanisms are introduced. To some extent, they can satisfy the need of security for the wireless sensor networks. But the severe constraints and demanding deployment environments of wireless sensor networks make computer security for these systems more challenging than for conventional networks. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack. Consequently, security and privacy pervade every aspect of system design. Ongoing direction is how to secure wireless communication links against eavesdropping, tampering, traffic analysis, and denial of service.

6. REFERENCES

[1] B. Krishnamashari, D. Estrin and S. Wicker, "Impact of Data Aggregation in Wireless Sensor Networks", *Proc. 22nd International Conference Distrib. Comp. Systems*, Jul. 2002, pp. 575-578.

[2] H. Luo, Y. Lin and S. K. Das, "Routing Correlated Data in Wireless Sensor Networks: A Survey", *IEEE Network*, vol. 21, no.6, Nov/Dec. 2007, pp. 40-47.

[3] Yoneki, E. & Bacon, J., (2005) "A survey of Wireless Sensor Network technologies: research trends and middleware's role", technical report. *http://www.cl.cam.ac.uk/TechReports,* ISSN 1476-2986.

[4] K. Lu et al., "A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks", *IEEE Transactions on Wireless Communications*, vol. 7, no. 2, Feb. 2008, pp. 639-647.

[5] R. Jiang and B. Chen, "Decision fusion with censored sensors", Proceedings of ICASSP, Vol. 2, Montreal, Canada, May 2004, pp. 289-292.

[6] Woo, A. and Culler, D., (2001) "A Transmission Control Scheme for Media Access in Sensor Networks", Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2001), Rome, Italy.

[7] D. Kazakos and P. Papantoni-Kazakos, Detection and Estimation, New York, USA: Computer Science Press, 1990.

[8] M. S. Kakasageri, S. S. Manvi and G. D. Sorgavi, "Agent-Based Information Access in Wireless Sensor Networks", WSEAS Transactions on Communications, vol. 3, no. 7, Jul. 2006, pp. 1369-1374.

[9] S. Rajasegarar, C. Leckie, and M. Palansiwami, "Anomaly detection in wireless sensor networks", IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp. 34-40.