ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

A Novel Security Issues Analysis and Evaluation of Security Method in WSNs

A.Senthilkumar[1], R.B.Saarooraj[2]

M.Tech (CSE)- Final Year, SRM University, Ramapuram, Chennai, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Science Engineering, SRM University, Ramapuram, Chennai, Tamil Nadu, India[2]

ABSTRACT: Wireless Sensor Networks (WSNs) are used in many applications in army, environmental, and healthcare related trust areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSNs. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. WSNs are often organized in challenging atmospheres where a competitor can substantially confinement some of the nodes, first can reprogram, and then, can duplicate them in a large number of emulations, easily taking control over the network. A few disseminated solutions have been recently proposed, but they are not adequate. First, they are energy and memory arduous: A serious drawback for any protocol to be used in the WSN resource constrained environment. First, we investigate the necessary properties of a dispersed mechanism for the detection of node reproduction spasms. Second, we show that the known resolutions for this problem do not finally meet our necessities. We proposed a new self-curative, randomized, efficient, and distributed protocol for the recognition of node duplication attacks, and we show that it gratifies the established requirements.

KEYWORDS: Wireless Sensor Networks, security requirements, key management protocol, security routing protocol.

I. INTRODUCTION

Recently the wireless communication and electronics have enabled the development of low-cost, low power, multi functional sensor nodes. These tiny sensor nodes, consisting of sensing, data processing, and communication components, make it possible to deploy Wireless Sensor Networks (WSNs), which represent a significant improvement over traditional wired sensor networks. WSNs can greatly simplify system design and operation, as the environment being monitored does not require the communication or energy infrastructure associated with wired networks..WSNs are expected to be solutions to many applications, such as detecting and tracking the passage of troops and tanks on a battlefield, monitoring environmental pollutants, measuring traffic flows on roads, and tracking the location of personnel in a building. Many sensor networks have mission-critical tasks and thus require that security be considered. Improper use of information or using forged information may cause unwanted information leakage and provide inaccurate results. While some aspects of WSNs are similar to traditional wireless ad hoc networks, important distinctions exist which greatly affect how security is achieved. The differences between sensor networks and ad hoc networks are:

- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures due to harsh environments and energy constraints.
- The topology of a sensor network changes very frequently due to failures or mobility.
- Sensor nodes are limited in computation, memory, and power resources.
- Sensor nodes may not have global identification.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

These differences greatly affect how secure data-transfer schemes are implemented in WSNs. For example, the use of radio transmission, along with the constraints of small size, low cost, and limited energy, make WSNs more susceptible to denial-of-service attacks. Advanced anti-jamming techniques such as frequency-hopping spread spectrum and physical tamper-proofing of nodes are generally impossible in a sensor network due to the requirements of greater design complexity and higher energy consumption. Furthermore, the limited energy and processing power of nodes makes the use of public key cryptography nearly impossible.

II.RELATED WORK

Namdeep Singh and Er. Jasvir Singh in July 2013 Public key cryptographic techniques provide more security as compare to symmetric key cryptographic techniques at the cost of more energy consumption and more resource utilization. The Hybrid cryptographic techniques have been developed for Wireless Sensor Networks (WSNs) for balancing energy consumption and security level. By using Hybrid cryptographic techniques few security frameworks have been proposed in past few years to provide more security and with less memory requirements. Bi Jiana and E Xu in 2013, proposed a security node-based key management protocol for cluster-based sensor networks. In this protocol generation of security nodes and different types of keys is described by the author. Performance analysis and simulation show that the by the proposed key management protocol energy consumption is less and key generation delay time is short. At the same time, more collaborative authentication security for keys is provided by the protocol. It can strongly recover against node capture, and can support large networks. Sai Ji, Liping Huang and Jin Wang in February 2013, proposed a novel key management scheme for the dynamic WSNs. In the network deployment phase, the security authentication and random key distribution were initialized. During the network stable phase, the scheme proposed a dynamic updated key based on the AVL tree in order to ensure the real-time update security for the network topology. Simulation results showed that this program can ensure the WSN's dynamic security as well as achieve the energy efficiency goal. Chia-Mu, Y., L. Chun-Shien, and K. Sy-Yen.- a protocol based on conflict, in which when the nodes n and node n can meet each other, both of them produce a random number and exchange them. Then the nodes store both received and sent numbers. If n and n meet again later, they swap the previously stored numbers and compare it with the numbers stored before and based on the comparison result can detect the attack .

III. SECURITY REQUIREMENTS

The main goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

- **Availability,** which ensures that the desired network services are available even in the presence of denial-of-service attacks.
- **Authorization,** which ensures that only authorized sensors can be involved in providing information to network services.
- **Authentication,** which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node.
- **Confidentiality**, which ensures that a given message cannot be understood by anyone other than the desired recipients.
- **Integrity,** which ensures that a message sent from one node to another is not modified by malicious intermediate nodes
- **Nonrepudiation**, which denotes that a node cannot deny sending a message it has previously sent.
- **Freshness,** which implies that the data is recent and ensures that no adversary can replay old messages.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Moreover, as new sensors are deployed and old sensors fail, we suggest that forward and backward secrecy should also be considered:

- Forward secrecy: a sensor should not be able to read any future messages after it leaves the network.
- Backward secrecy: a joining sensor should not be able to read any previously transmitted message.

The security services in WSNs are usually centered around cryptography. However, due to the constraints in WSNs, many already existing secure algorithms are not practical for use.

IV. APPLICATIONS OF WIRELESS SENSOR NETWORK

Wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems. The rapid deployment, self-organization and fault tolerance characteristics of sensor networks make them a very promising sensing technique for military. Since sensor networks are based on the dense deployment of disposable and low-cost sensor nodes, destruction of some nodes by hostile actions does not affect a military operation as much as the destruction of a traditional sensor, which makes sensor networks concept a better approach for battlefields. Some of the military applications of sensor networks are monitoring friendly forces, equipment and ammunition; battle field surveillance; reconnaissance of opposing forces and terrain; targeting; battle damage assessment and nuclear, biological and chemical.

- **Environmental applications-**Forest fire detection: Since sensor nodes may be strategically, randomly, and densely deployed in a forest, sensor nodes can relay the exact origin of the fire to the end users before the fire is spread uncontrollable. Millions of sensor nodes can be deployed and integrated using radio frequencies/ optical systems. Also, they may be equipped with effective power scavenging methods, such as solar cells, because the sensors may be left unattended for months and even years. The sensor nodes will collaborate with each other to perform distributed sensing and overcome obstacles, such as trees and rocks, that block wired sensors' line of sight. (NBC) attack detection and reconnaissance.

- **Healthcare applications-**Some of the healthcare applications for sensor networks are providing interfaces for the disabled ;integrated patient monitoring; diagnostics; drug administration in hospitals; monitoring the movements and internal processes of insects or other small animals; telemonitoring of human physiological data and tracking and monitoring doctors and patients inside a hospital. Tracking and monitoring doctors and patients inside a hospital: Each patient has small and lightweight sensor nodes attached to them. Each sensor node has its specific task. For example, one sensor node may be detecting the heart rate while another is detecting the blood pressure. Doctors may also carry a sensor node, which allows other doctors to locate them within the hospital. Drug administration in hospitals: If sensor nodes can be attached to medications, the chance of getting and prescribing the wrong medication to patients can be minimized. Because, patients will have sensor nodes that identify their allergies and required medications. Computerized systems as described that they can help minimize adverse drug events.

- **Home applications-**Interactive museums: In the future, children will be able to interact with objects in museums to learn more about them. These objects will be able to respond to their touch and speech. Also, children can participate in real time cause-and-effect experiments, which can teach them about science and environment. In addition, the wireless sensor networks can provide paging and localization inside the museum. Detecting and monitoring car thefts: Sensor nodes are being deployed to detect and identify threats within a geographic region and report these threats to remote end users by the Internet for analysis .Managing inventory control: Each item in a warehouse may have a sensor node attached. The end users can find out the exact location of the item and tally the number of items in the same category. If the end users want to insert new inventories all the users need to do is to attach the appropriate sensor nodes to the inventories. The end users can track and locate where the inventories are at all times.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

V. PUBLIC KEY CRYPTOGRAPHY IN WSN'S

Public key algorithms such as RSA are computationally intensive and usually execute thousands or even millions of multiplication instructions to perform a single security operation. Further, a microprocessor's public key algorithm efficiency is primarily determined by the number of clock cycles required to perform a multiply instruction. Brown et al.found that public key algorithms such as RSA usually require on the order of tens of seconds and up to minutes to perform encryption and decryption operations in constrained wireless devices which exposes a vulnerability to DoS attacks. On the other hand, Carman et al. found that it usually takes a microprocessor thousands of nanojoules to do a simple multiply functions with a 128 bit result. In contrast, symmetric key cryptography algorithms and hash functions consume much less computational energy than public key algorithms.

VI. KEY MANAGEMENT PROTOCOLS APPROACHES

- **Deterministic Approaches**-An individual key shared with the base station (pre distributed). A group key that is shared by all the nodes in the network (pre distributed),.Pairwise keys shared with immediate neighboring nodes.

- **Probabilistic Approaches** — Most of the proposed key management schemes in WSNs are probabilistic and distributed schemes. We introduced a key pre distribution scheme for sensor networks which relies on probabilistic key sharing among the nodes of a random graph. This scheme consists of three phases:

  - **Key Predistribution Phases**- In the key pre distribution phase, each sensor is equipped with a key ring held in the memory. The key ring consists of k keys which are randomly drawn from a large pool of P keys. The association information of the key identifiers in the key ring and sensor identifier is also stored at the base station. Further, the authors assumed that each sensor shares a pair wise key with the base station.

  - **Shared Key Discovery Phases**- In the shared key discovery phase, each sensor discovers its neighbors within the wireless communication range with which it shares keys. The simplest method is for each node to broadcast a list of identifiers of the keys in their key ring in plain text, thus allowing neighboring nodes to check whether they share a key. However, an adversary may observe the key-sharing patterns among sensors in this way. The second method uses the challenge–response technique to hide key-sharing patterns among nodes from an adversary. For every Ki on a key ring, each node could broadcast a list. The decryption of with the proper key by a recipient would reveal the challenge and establish a shared key with the broad casting node. This method requires that well known in the sensor network, thus allowing the recipient with the proper key to discover the challenge.

  - **Path Key Establishment Phase**-In the path-key establishment phase, a path-key is assigned for those sensor nodes within wireless communication range and not sharing a key, but connected by two or more links at the end of the second phase. If a node is compromised the base station can send a message to all other sensors to revoke the compromised node's key ring. Rekeying follows the same procedure as revocation. The messages from the base station are signed by the pair wise key shared by the base station and sensor nodes, and thus it is ensured that no adversary can forge a base station.

VII. THREAT MODEL

In WSNs, it is usually assumed that an attacker may know the security mechanisms that are deployed in a sensor network; they may be able to compromise a node or even physically capture a node. Due to the high cost of deploying tamper resistant sensor nodes, most WSN nodes are viewed as non tamper-resistant. Further, once a node is compromised, the attacker is capable of stealing the key materials contained within that node. It can compromise a certain fixed amount of nodes and replicate one or more into multiple copies (the clones). In general, to cope with this threat, it could be possible to assume that nodes are tamper-proof. However, tamper-proof hardware is expensive and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

energy demanding. Therefore, consistently with a large part of the literature, we will assume that the nodes do not have tamper-proof components. The adversary goal is to prevent clones from being detected by the detection protocol used in the network. Hence, we assume that the adversary, to reach its goal, also tries to subvert the nodes that will possibly act as witnesses. Base stations in WSNs are usually regarded as trustworthy. Most research studies focus on secure routing between sensors and the base station. Deng *et al.* considered strategies against threats which can lead to the failure of the base station. Attacks in sensor networks can be classified into the following categories:

• **Outsider versus insider attacks:** outside attacks are defined as attacks from nodes which do not belong to a WSN; insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways.

• **Passive versus active attacks:** passive attacks include eavesdropping on or monitoring packets exchanged within a WSN; active attacks involve some modifications of the data steam or the creation of a false stream.

• **Mote-class versus laptop-class attacks**: in mote-class attacks, an adversary attacks a WSN by using a few nodes with similar capabilities to the network nodes; in laptop-class attacks, an adversary can use more powerful devices (e.g., a laptop) to attack a WSN. These devices have greater transmission range, processing power, and energy reserves than the network nodes.

VIII.SIMULATION RESULTS

For analyzing key management method and comparing this method with other works, the method is simulated using .Net Framework technology and ASP.NET programming language. The WSN simulator of is used for this method. The simulation results are evaluated based on the energy consumption and the number of performed comparisons. Table 1.Simulation Parameters indicates parameters used in this simulation. The test wireless network is constructed and simulated 30 times. In 15 experiments the networks are constructed with 50 nodes and in the other 15 experiments the networks are constructed with 100 nodes. In each simulation run, a single node is selected randomly . In all experiments 10 percent of nodes are selected as the agent nodes. Energy in wireless sensor networks is a critical issue, to estimate the expended energy in sensor nodes.

Table 1.Simulation Parameters

Symbol	**Meaning**
Network scale	100m *100m
Transmission range	25m
Energy	A,B
Speed	10ms

IX. EVALUATION OF SECURITY SCHEME IN WSNs

We suggest using the following metrics to assess whether a security scheme is appropriate in WSNs.

• **Security:** A security scheme has to meet the requirements

.

• **Resiliency**: In case a few nodes are compromised, a security scheme should still protect against the attacks.

• **Energy efficiency:** A security scheme must be energy efficient so as to maximize node and network lifetime.

• **Flexibility:** Key management needs to be flexible so as to allow for different network deployment methods, such as random node scattering and predetermined node placement.

Scalability: A security scheme should be able to scale without compromising the security requirements.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

• **Fault-tolerance:** A security scheme should continue to provide security services in the presence of faults such as failed nodes.

• **Self-healing:** Sensors may fail or run out of energy. The remaining sensors may need to be reorganized to maintain a set level of security.

• **Assurance:** Assurance is the ability to disseminate different information at different levels to end-users. A security scheme should offer choices with regard to desired reliability, latency, and so on.

X. CONCLUSION AND FUTURE DIRECTION

Security in wireless sensor networks is a novel trust of research areas, with a limited, but rapidly growing set of research results. This paper includes security issues and challenges and assessment of security schemes, key management protocol, security routing protocol and threat model to the sensor networks which may be helpful in order to implement security mechanism. Through this paper, the researchers can understand all the security requirements and threats that affect the WSN and researchers can also find out new attacks which affect the WSN security. As WSNs grow in capability and are used more frequently, the need for security in them becomes more apparent. However, the nature of nodes in WSNs gives rise to constraints such as limited energy, processing capability, and storage capacity. These constraints make WSNs very different from traditional ad hoc wireless networks. As such, special protocols and techniques have been developed for use in WSNs. While discussed security in wireless networks, none focus specifically on security in WSNs and the constraints unique to them. In this article, we have surveyed the security issues in WSNs starting with the attacks and countermeasures in each network layer followed by the issues and solutions in cryptography, key management finally secure routing, While the discussed security services certainly add more computation, communication, and storage overhead in WSNs, and thus consume more energy, they are highly desirable and often required in real-world applications.

WSNs are promising solutions for many applications and security is often a key concern. Although research efforts have been made with regard to cryptography, key management, secure routing, secure data in WSNs, there are still some challenges to be addressed. First, the selection of the appropriate cryptographic methods depends on the processing capability of sensor nodes, indicating that there is no unified solution for all sensor networks. Instead, the security mechanisms are highly application-specific. Second, sensors are characterized by the constraints on energy, computation capability, memory, and communication bandwidth. The design of security services in WSNs must satisfy these constraints. Third, most of the current protocols assume that the sensor nodes and the base station are stationary. However, there may be situations, such as battlefield environments, where the base station and possibly the sensors need to be mobile. The mobility of sensor nodes has a great influence on sensor network topology and thus raises many issues about secure routing protocols. In particular, we identify some of the future directions in the study of security issues in WSNs as follows. Exploit the availability of private key operations on sensor nodes: Recent studies on public key cryptography show that public key operations may be practical in sensor nodes. However, private key operations are still too expensive to accomplish in a sensor node. As public key cryptography can greatly ease the design of security in WSNs, improving the efficiency of private key operations on sensor nodes is highly desirable. Secure routing protocols for mobile sensor networks: The mobility of sensor nodes has a great influence on sensor network topology and thus on the routing protocols. Mobility can be at the base station, sensor nodes, or both. Current protocols assume the sensor network is stationary. New secure routing protocols for mobile sensor networks need to be developed. Continuous stream security in WSNs: Recent work on security in sensor networks focuses on discrete events such as temperature and humidity. Continuous stream events such as video and images are not discussed. Video and image sensors for WSNs might not be widely available now, but will likely be in the future. Substantial differences in authentication and encryption exist between discrete events and continuous events, indicating that there will be distinctions between continuous stream security and the current protocols in WSNs. QoS and security performance is generally degraded with the addition of security services in WSNs. Modern studies on security in WSNs focus on individual topics such as key management, secure routing. QoS and security services need to be evaluated together in WSNs.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

REFERENCES

[1].Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security & Privacy Special Issue: Making Wireless Work, vol. 2, no. 3, May/June 2004, pp. 28–39.
[2] D. Djenouri, L. Khelladi, and N. Badache, "A Survey on Security Issues in Mobile Ad Hoc and Sensor Networks," IEEE Commun.Surveys and Tutorials, vol. 7, no. 4, 2005.
[3] Wireless sensor networks: a survey-I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci- Computer Networks 38 (2002) 393–422.
[4]. Sudhir Agarwal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in WSN" Journal of Computing, Vol. 3, Issue 1, ISSN- 2151-9617, 2011.
[5] Chaudhari H.C. and Kadam "Wireless Sensor Networks: Security, Attacks and Challenges" L.U. International Journal of Networking Volume 1, Issue 1, 2011, pp-04-16 .
[6] Al-Sakib khan Pathan, "Security in wireless sensor networks: Issues and challenges", ICACT2006, ISBN 89-5519-129-4, pp-1043-1048.
[7] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, "Sensor Network Security: A Survey", IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, Second quarter 2009, pp. 52-73.
[8] Yong Wang, Garhan Attebury, And Byrav Ramamurthy, "A Survey Of Security Issues In Wireless Sensor Networks" , IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter 2006.
[9] Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, "Security in Wireless Sensor Networks: Issues and Challanges", Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace) 2013, Malaysia, ISSN: 2165-4301, pp. 356-360.
[10] Sunil Ghildiyal, Ashish Gupta, Musheer Vaqur, Anupam Semwal, "Analysis of Wireless Sensor Networks: Security, Attacks and Challenges", IJRET, Volume 3, Issue 3, eISSN: 2319-1163, pp. 160-164.
[11].Namdeep Singh, Er. Jasvir Singh, "A Security Framework for Wireless Sensor Networks", Journal of Global Research in Computer Science, Volume 4, No. 7, July 2013.
[12] Bi Jiana, E Xu, "An Energy-efficient Security Node-based Key Management Protocol for WSN", Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation, 2013.
[13] Sai Ji, Liping Huang and Jin Wang, "A Novel Key Management Scheme Supporting Network Dynamic Update in Wireless Sensor Network", International Journal of Grid and Distributed Computing Vol. 6, No. 1, February, 2013.