Evaluation of Issues in WSN and Implementation of Distance Vector Routing

Shivani Chaudhary[1] Atul Kumar[2]

[1,2]KIIT College of Engineering Gurugram, India

Abstract— Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. These networks will consist of hundreds or thousands of self-organizing, low power, low-cost wireless nodes deployed to monitor and affect the environment. Security is becoming a major concern for WSN protocol designers because of the wide security-critical applications of WSNs. In this article we discuss some basic information about the WSN and highlights ongoing research activities and issues that affect the design and performance of Wireless Sensor Network. This paper presents some challenges related to Security of Wireless Sensor Networks and Implementation of Distance Vector Routing Algorithm.

Key words: WSN, Cryptography, Topology

I. Introduction

Wireless sensor network consist of hundreds or even thousands of small devices to monitor the real-world environment each with sensing, processing, and communication capabilities. These networks will consist of hundreds or thousands of self-organizing, low power, low-cost wireless nodes deployed to monitor and affect the environment. Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. The communication among the sensors is done using wireless transceivers in wireless sensor networks. Sensor networks concern to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements [1].This leads to a very demanding environment to provide security.

A Wireless Sensor Network is a combination of wireless networking and embedded system technology that monitors physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Security has a great importance in Wireless Sensor Network. For example, when sensor network is used for military purpose, it is very important to keep the sensed information confidential and authentic.

In this article, we present a study of security in WSN. We discuss some issues and challenges in Wireless Sensor Network in this paper. To address the critical security issues in wireless sensor networks we talk about cryptography, and other basics of network security and their applicability [2]. We explore various types of threats and attacks against wireless sensor network. We review the related works and proposed schemes concerning security in WSN. Finally we conclude the paper delineating the research in wireless sensor network security. In section 2 we have presented security mechanisms. Section 3 we have discussed the design issue and section 6 presents implementation of distance vector outing algorithm. Finally we presents result and analysis distance vector routing algorithm.

II. Security Mechanisms for Wireless Sensor Networks

A. Cryptography

Cryptography schemes are often utilized to meet the basic security requirements of confidentiality and integrity in networks. But as the sensor nodes are limited in their computational and memory capabilities, the well-known traditional cryptographic techniques cannot be simply transferred to WSNs without adapting them.

B. Symmetric Cryptographic

In symmetric cryptographic techniques, a single shared key is used between the two communicating nodes both for encryption and decryption. This key has to be kept secret in the network, which can be quite hard in the exposed environment where WSNs are used. Most security schemes for WSN use only symmetric cryptography, due to its ease of implementation on limited hardware and small energy demands, especially if he implementation is done in hardware to minimize performance loss. [4] Two types of symmetric ciphers are used: block ciphers that work on blocks of a specific length and stream ciphers that work bitwise on the data. A steam cipher can be seen as a block cipher with a block length of 1 bit.

C. Asymmetric Cryptographic Techniques

In asymmetric cryptography, a private key can be used to decrypt and sign data while a public key can be used to encrypt and verify data. The private key needs to be kept confidential while the public key can be published freely. Asymmetric cryptography is also known as Public key cryptography.

There are various public key algorithms include Rabin's Scheme, Ntru-Encrypt, RSA, Elliptic Curve Cryptography (ECC), Pairing Based Cryptography (PBC) and Identity Based Encryption.

D. Hybrid Cryptographic Techniques

Symmetric and asymmetric cryptography can be applied in combination to join the advantages of both approaches. Pugliese and Santucci, 2008discussed a novel hybrid cryptographic scheme for the generation of pairwise network topology authenticated keys (TAK) in WSNs, which is based on vector algebra in GF(q). Symmetric is used for ciphering and authentication, while asymmetric is used for key generation.

III. Previous work

A. A Survey on Measures for Secure Routing in Wireless Sensor Networks

WSN has become a major technology for sensing in various application areas. One of the main challenges in WSN is the safe route of data through a network. This is generated by the fact that WSN is normally deployed in unpredictable or even hostile environments. In the last few years, routing approaches were mainly focusing on metrics like robustness, energy conservation etc. Recently, various security solutions had come up, which kept security issues in WSN. In this paper, various types of attacks are examined on the WSN routing layer. After this, measures for the secure routing; Cryptography, key establishment, trust & reputation and secure localization; are reviewed, which were proposed by researchers in this area.

B. A Light Weight Cryptographic Hash Algorithm for Wireless Sensor Network

The authentication of a message is a great research challenge in today's advanced wires and wireless communications. Cryptographic hash functions are used to protect the authenticity of the information. Some of the most popular and commonly used cryptographic hash algorithms are MD5 and SHA1. These hash algorithms are used in a variety of security applications, e.g. securing node/message in traditional networks.

C. Study of Security in Wireless Sensor Networks

Wireless Sensor Network (WSN) is emerging technique that shows great assurance for future Application for both public and military. Many researchers tried to develop further cost and energy-efficient computing devices and algorithms for WSN. However, Security is important for the success of implementing WSN. Security becomes extremely important, as they are prone to different types of despite attacks. The intent of this paper is to investigate security problems and various security requirements. We identify the attacks at all the layers of WSN network architecture and also tried to find their possible solution.

IV. Issues in Wireless Sensor Network

A. Design Issues

Fault –tolerant Communication: Due to the deployment of sensor nodes in an uncontrolled environment, it is not uncommon for the sensor nodes to become faulty and unreliable. Low latency: The events that work with the framework are essential that should be identified immediately by the operator. Therefore, the framework is to identify and inform events as soon as possible.

Scalability: A system, whose performance improves after adding hardware, proportionally to the capacity added, is said to be a scalable system. The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more.

Transmission Media: In a multi-hop sensor network, communicating nodes are linked by a wireless medium. [5] The traditional problems associated with a wireless channel may also affect the operation of the sensor network. Coverage Problems: It reflects the quality of service that can be provided by a particular sensor network.

B. Topology Issues

Geographic routing: The geographical routing is a routing principle that depends on the geographical position Information. This is mainly proposed for the wireless network and based on the idea that the source sends message to the geographical location of the destination instead of using the network address. Sensor Hole: A routing hole is an area in the sensor network, where the nodes are not available or available nodes cannot participate in actual routing of data due to various reasons. The task of identifying holes is particularly challenging because the specific wireless sensor networks are involved lightweight, low-capacity nodes that are unaware of their geographical location. Coverage Topology: Coverage problem reflects how well an area is monitored or tracked by sensors.

V. Challenges of Wireless Sensor Network

- Energy Efficiency
- Limited storage and computation
- Low bandwidth and high error rates
- Errors are common — Wireless communication — Noisy measurements — Node failure are expected
- Scalability to a large number of sensor nodes

VI. Implementation of Distance Vector Routing Algorithm

Router transmits its distance vector to each of its neighbors in a routing packet.

Each router receives and saves the most recently received distance vector from each of its neighbors.

A router recalculates its distance vector when:

It receives a distance vector from a neighbor containing different information than before.

It discovers that a link to a neighbor has gone down.

The DV calculation is based on minimizing the cost to each destination

Dx(y) = Estimate of least cost from x to y

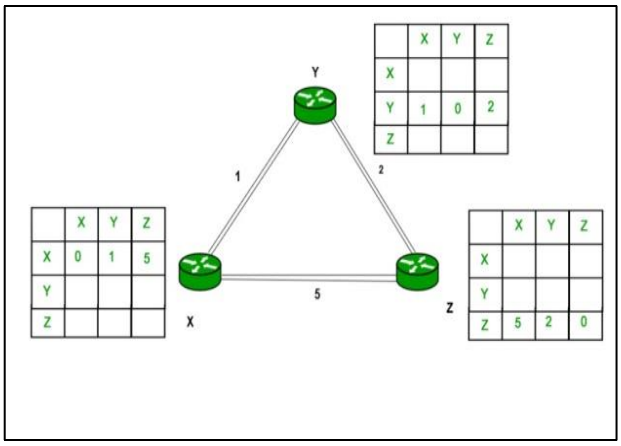
C(x,v) = Node x knows cost to each neighbor v

Dx = [Dx(y): y ∈ N] = Node x maintains distance vector

Node x also maintains its neighbors' distance vectors

– For each neighbor v, x maintains Dv = [Dv(y): y ∈ N]

Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.

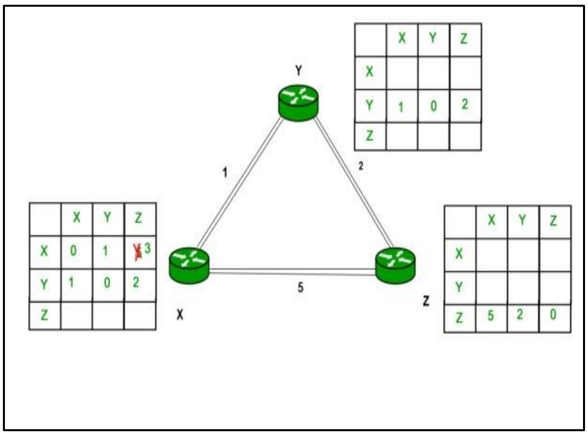


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	5
Y			
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Fig. 6.1: Routing Table X



	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

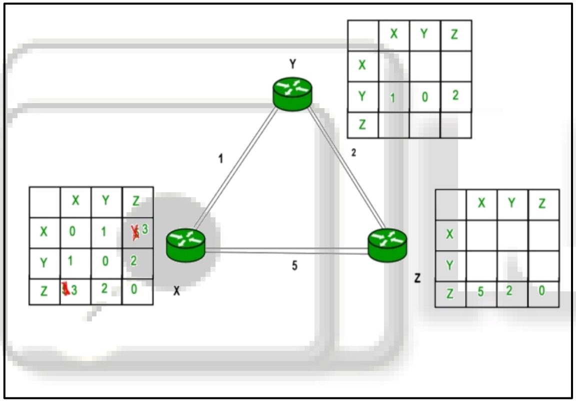
Fig. 6.2: Routing Table Y

Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

$$D_x(y) = \min \{ C(x,v) + D_v(y)\} \text{ for each node } y \in N$$

As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.

Similarly for Z also –

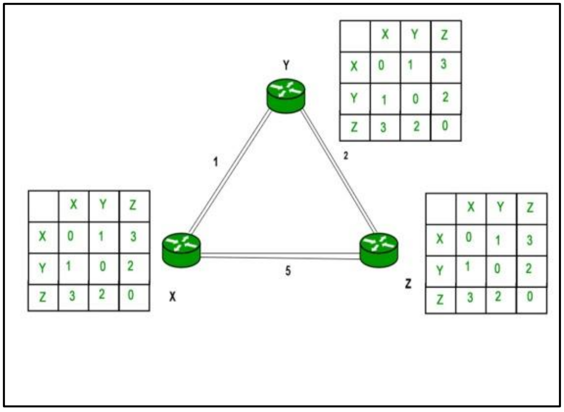


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z	~~5~~ 3	2	0

	X	Y	Z
X			
Y			
Z	5	2	0

Fig. 3: Routing Table Z



	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

Fig. 4: Final Routing Table F

VII. CONCLUSION

Wireless sensor networks consist of small nodes with sensing, computation, and wireless communications capabilities. Many routing, power management, and data dissemination protocols are specially designed For WSN. The wireless sensor networks continue to grow and become widely used in many applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, etc. There are many ways to provide security, one is cryptography. Selecting the appropriate cryptography method for sensor nodes is fundamental to provide security services in WSNs.[6] Public Key based cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches. Finally we have proposed the Distance Vector Routing Algorithm for its implementation.

Wireless sensor networks are still a young research field. There is still a lot of activity going on to solve many open issues.WSN is a very important tool for making our life comfortable and safe.

REFERENCES

[1] Jaydip Sen “Security in Wireless Sensor Networks”In International Journal of Communication Networks and Information Security (IJCNIS) Vol 2 Issue 1 pp59-82 (2010)

[2] Madhumita Panda “Security in Wireless Sensor Networks using Cryptographic Techniques” In American Journal of Engineering Research (AJER) Volume-03, Issue-01, pp-50-56 (2014)

[3] T.Kavitha , D.Sridharan,“Security Vulnerabilities In Wireless Sensor Networks: A Survey” In Journal of Information Assurance and Security 5 031-044 (2010).

[4] Khushboo Gupta P“Design Issues and Challenges in Wireless Sensor Networks” In International Journal of Computer Applications (0975 – 8887) Volume 112 – No 4, February 2015.

[5] Indu, Sunita Dixit, “Wireless Sensor Networks: Issues & Challenges” In International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, , pg. 681-685 June-(2014).

[6] Sadaqat Ur Rehman, Muhammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah, Obaid Ur Rehman,“ Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)” In International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, (2012)

[7] Prasanth Ganesan, Ramnath Venugopalan ,Pushkin Peddabachagari, Alexander Dean,Frank Mueller and Mihail Sichitiu, “Analyzing and modelling encryption overhead for sensor network nodes” In Proceeding of the Ist ACM international workshop on Wireless sensor networks and application, San Diego, California, USA, September (2003).

[8] Ling Tan, Shunyi Zhang, and Yanfeng Sun, Jing Qi,“Application of Wireless Sensor Networks in Energy Automation‖, Sustainable Power Generation and Supply, In International conference Supergen’09 2009.

[9] Yee Wei Law, Jeroen Doumen and Pieter Hartel “Survey and benchmark of block ciphers for wireless sensor networks” In ACM Transactions on Sensor Networks(TOSN),2(2006),65-93.