Adaptive Security in Wireless Sensor Networks

C.Sasikala[1], Dr. A. Senthilkumaran[2]

[1]*(Research scholar, Department of Computer science, Bharathiyar University ,Coimbatore.)*
[2]*(Associate Professor Department of Computer science Arignar Anna Government Arts and Science college Nammakkal.)*

Abstract: *Wireless sensor networks (WSNs) have been deployed into a variety of applications including military system and homeland security. Wireless network can perform multipath routing in short distance to save energy and a power of particular mode. Some security issues, threats and attacks, security framework were discussed in this paper. Classification of routing protocol and adaptive security provision were also discussed in the paper.*

Keywords: *WSN (Wireless Sensor Network), Routing Protocol, Adaptive Security Provision*

I. Introduction

WSN is a combination of many small sensors [7]. These sensor nodes combined with one to another sensor / base station. Sensor are nodes which perform some kinds of task such as data processing, compound communication.

Characteristics :

- Reduced power
- Reduced bandwidth
- Minimum size
- Low energy

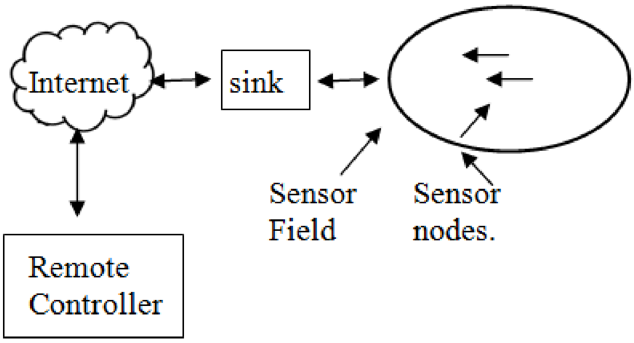

Fig (i): Wireless Sensor Network Model

The above figure explains in detail about the wireless sensor network model[4]. It consist of one sink node, internet connection, remote controller and WSN nodes. The WSN nodes have many number of sensor nodes and sensor field. The sink is also known as base station. A large number of sensor nodes are deployed over a large geographic area or sensor field. Data are transferred from sensor nodes to sink through multi-hop communication model.

Application of sensor Network:

- They are used in military application for guiding the system of intelligent missiles, and finding the attack by weapons etc.
- In forest for controlling fire and air and water pollution.
- In patient body for diagnosis and monitoring.
- In industries for observing & conservation of machines & finding emergencies.

II. Security Framework For WSN

Threats & attacks [4] have been identified and analyzed together with some key security requirements to be able to define the security policies & adaptive security framework for WSN have been identified.

Threats & attacks :

Key threat in WSN are given below.

1. Sensor mode compromise
2. Eavesdropping
3. Privacy of sensed data
4. Denial of service attack

Security issues in sensor network

Sensor Network have several constraints involving battery power, working memory, transmission range, recharge ability, sleep patterns, etc.

III. Routing Protocols Classification

Routing protocols [5], [6] in WSN was classified into 3 major types. They are

1. Flat based / data centric
2. Hierarchical based / clustering
3. Location based.

1. Flat – based :

Flat routing protocol is a network communications protocol created by routers in which all are each other's peers. It distributes routing information to routers that are connected to each other.

This is further classified into 5 categories. They are flooding and gossiping, spin, direct diffusion, energy aware routing and energy efficient geocast routing. It is also called data centric protocol.

2. Hierarchical based :

Hierarchical routing is the procedure of arranging routers in a hierarchical manner. It is also called clustering.

Clustering is classified into 4 types. They are LEACH & TL-LEACH, PEGASIS & H-PAGASIS, TEEN & APTEEN and HEED.

3. Location based routing

Location information contains distance between two different modes for routing data. Distance is calculated on the basis of signal strength so that energy consumption is calculated.

There are 3 major types in location based. They are MECN, GEAR and GAF/H-GAF

IV. Adaptive Security Provisions

The adaptive security architecture distinguish these devices into trusted and non-trusted devices. The trusted device has no restricted access to all services. Three security nodes are proposed for a non- trusted device. They are low – level, medium – level and high – level security.

Each security services (such as integrity, confidentially and authentication) can be realized using various security mechanisms. Adaptable security nodes often called quality of protection (QoP) models[1], [3], allows the calculation of different variation of the mechanism that protects the transmitted data, achieving different security levels.

This depends on the parameters such as,

- Parameters of used cryptographic element.
- Importance of protected content
- Message priority.
- Probability of an attack.
- Assets gained during successful attack.

The QoP model uses the following three primary parameters.

1. L : the protection level
2. P : the probability of an incident occurrence
3. W : the impact of a successful attack.

The security provision [2] proposed here is under two ways: dust and energy aware route setup and rotation of selected data paths. The energy factor is the link cost function issued in convention method is:

$$\text{Cost}_{ij} = c\,(\text{dist}_{ij})^l$$

The cost of a path is given by,

$$\text{Cost}_{path}=\underset{i\in path}{\text{Energy}}\,(\text{mins}\,(\text{Trust})) + \sum_{ij\in path} c_o\,(\text{dist}_{ij})^l$$

where dist_{ij} is the distance between the modes i,j,c is a constant and the parameter l depends on the environment and approximately equals to 2 and Energy() reflects the energy consumed in encrypting packets.

V. Implementation

The ASP approach is validated through simulation (using NS2 simulators) several protocols like Dynamic source routing (DSR), Ad-hoc On- Demand Distance. Vector Routing (AODV) and Destination – Sequenced Distance – Vector (DSDV) are implemented in NS2.

VI. Conclusion

In recent years, wireless sensor network are under usage in security – sensitive application such as border protection, digital battlefields, etc. ASP employs a path rotation to prevent from defecting the cryptosystem used in trusted path. Routing with energy awareness is latest topic in research to increase the network lifetime and performance. In future, Routing Algorithm by considering power aware metrics like link cost, transmission time, data reliability etc.

References

[1]. Kalpana Sharma, M.K. Ghose, Kuldeep, "complete security Framework for wireless sensor networks", *International Journal of computer science and Information security*.

[2]. Mohammed Younis and Nick Krajewski, "Adaptive Security provision for increased energy efficiency in WSN*", IEEE International workshop. On WLN 2009*

[3]. "*Towards Adaptable Security for energy efficiency is WSN"* by Nikos Fotiou, Giamnis F. Marias, Wireless World Research forum 2012.

[4]. K. Sivakumar, Dr. T. Ravichandiran, "Security Framework for wireless sensor, Networks", *Journal of computer applications.*

[5]. Aphrin S. patham, Shabda Dongakar, "Algorithm to increase energy efficiency and coverage for wireless sensor network", *International Journal of science and Research.*

[6]. Rajashree. V. Birdar , V. C. Patil, Dr. S. R. Sawant, "*Classification and comparison of routing protocols in wireless sensor networs", Special issue on Ubiquitious computing security systems.*

[7]. "Security and efficient data collection in WSN ", Gurupreet Kaur, Navdeep Kumar in "*International Journal of Advanced Research in computer science and software engineering"*

One Day National Conference On "Internet Of Things - The Current Trend In Connected World" NCIOT-2018 38 | Page