International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue 07, July 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

SECURE LOCALIZATION IN WIRELESS SENSOR NETWORK

Renu Kumari[1], Sachin Shrivastava[2]

[1]M.Tech Student, [2] Assistant Professor, Department of Computer Science & Engineering, SCET, Palwal (India)

ABSTRACT

Wireless sensor networks are about the field of networks that consists of small, large number of sensing nodes which is having the sensing, computational and transmission power but sensing nodes also suffer from many limitation such as low power (usually operated by battery), low processing ability, communication and storage limitations. The tiny nodes are deployed in target areas according to the deployment nature of target but nodes are easily targeted by attacker with physical attack of node capture. So, secure communications in some wireless sensor networks are critical because these networks are highly vulnerable to internal and external attacks. In our thesis, we present an enhanced ***High-Resolution Robust Localization*** *for security of wireless sensor networks. This combination of scheme provides the good performances and efficiency in terms of network connectivity, key storage overhead as well as in terms of attack of node capture. In the end we compared our scheme with Existing schemes and our scheme gives better security and performances.*

I. INTRODUCTION

A wireless sensor network, consisting of a large number of small low cost devices called sensor nodes or motes. A sensor node is contained information about the battery transceiver, micro-controller and sensors. These sensor nodes are tiny resource constrain devices with the limitations of low battery power and communication range and small computation and storage capabilities. They are usually deployed in open environments where they collaboratively monitor the physical and environmental data such as temperature, pressure vibration etc., and report/relay the sensed data to other sensor nodes over a wireless network. The final destination of this data is a base station also called a sink node which is a powerful device, e.g., a laptop. The base station acts as a gateway and links the WSN to the outer network e.g., the Internet as shown in Figure 1.1.

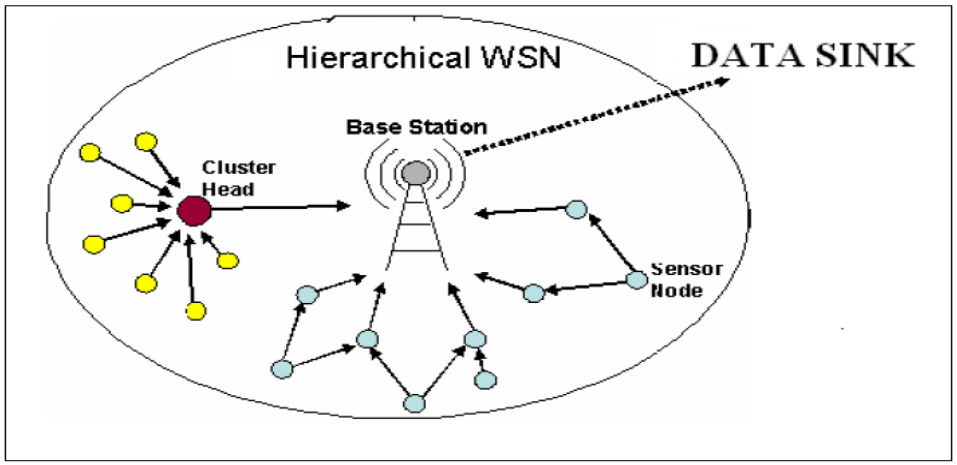

Figure 1.1: Base station (sink node)

1.2 Applications of Wireless Sensor Networks

Sensor networks are tools to bridge the gap between the physical and the virtual world.

They allow automatically collecting information about physical phenomena, immediately processing this information and transferring the results into background information systems. This processing delivers high-level information according to the applications requirements. Sensor nodes organize themselves autonomously, work in a collaborative manner, and are designed for energy efficiency. This allows it to monitor large geographical areas or inaccessible spaces over long periods of time without the need of human intervention[1][2].

1.2.1 Military Applications

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 C4ISRT. 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[3]. Some of the military applications of sensor networks are monitoring friendly forces, equipment and ammunition; battlefield surveillance; reconnaissance of opposing forces and terrain; targeting; battle damage assessment nuclear, biological and chemical (NBC) attack detection and reconnaissance.

Monitoring friendly forces, equipment and ammunition: Leaders and commanders can constantly monitor the status of friendly troops, the condition and the availability of the equipment and the ammunition in a battlefield by the use of sensor networks. Every troop, vehicle, equipment and critical ammunition can be attached with small sensors that report the status. These reports are gathered in sink nodes and sent to the troop leaders. The data can also be forwarded to the upper levels of the command hierarchy while being aggregated with the data from other units at each level [4].

Battlefield surveillance: Critical terrains, approach routes, paths and straits can be rapidly covered with sensor networks and closely watched for the activities of the opposing forces. As the operations evolve and new operational plans are prepared, new sensor networks can be deployed anytime for battlefield surveillance.

Reconnaissance of opposing forces and terrain: Sensor networks can be deployed in critical terrains, and some valuable, detailed, and timely intelligence about the opposing forces and terrain can be gathered within minutes before the opposing forces can intercept them.

Targeting: Sensor networks can be incorporated into guidance systems of the intelligent ammunition.

Battle damage assessment: Just before or after attacks, sensor networks can be deployed in the target area to gather the battle damage assessment data.

Nuclear, biological and chemical attack detection and reconnaissance: In chemical and biological warfare, being close to ground zero is important for timely and accurate detection of the agents. Sensor networks deployed in the friendly region and used as a chemical or biological warning system can provide the friendly forces with critical reaction time, which drops casualties drastically. We can also use sensor networks for detailed reconnaissance after an NBC attack is detected. For instance, we can make a nuclear reconnaissance without exposing a race team to nuclear radiation.

1.2.2 Environment Applications

Some environmental applications of sensor networks include tracking the movements of birds, small animals, and insects; monitoring environmental conditions that affect crops and livestock irrigation macro instruments for large-scale Earth monitoring and planetary exploration; chemical/biological detection; precision agriculture; biological, Earth, and environmental monitoring in marine, soil, and atmospheric contexts; forest fire detection; meteorological or geophysical research; flood detection; bio-complexity mapping of the environment; and pollution study.

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.

Bio complexity mapping of the environment: A bio complexity mapping of the environment requires sophisticated approaches to integrate information across temporal and spatial scales. The advances of technology in the remote sensing and automated data collection have enabled higher spatial, spectral, and temporal resolution at a geometrically declining cost per unit area. Along with these advances, the sensor nodes also have the ability to connect with the Internet, which allows remote users to control, monitor and observe the bio complexity of the environment.

Although satellite and airborne sensors are useful in observing large biodiversity, e.g., spatial complexity of dominant plant species, they are not fine grain enough to observe small size biodiversity, which makes up most of the biodiversity in an ecosystem. As a result, there is a need for ground level deployment of wireless sensor nodes to observe the bio complexity. One example of bio complexity mapping of the environment is done at the James Reserve in Southern California. Three monitoring grids with each having 25–100 sensor nodes will be implemented for fixed view multimedia and environmental sensor data loggers.

Precision Agriculture: Some of the benefits are the ability to monitor the pesticides level in the drinking water, the level of soil erosion, and the level of air pollution in real time.

1.2.3 Health Applications

Some of the health 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; tele monitoring of human physiological data; and tracking and monitoring doctors and patients inside a hospital.

Tele monitoring of human physiological data: The physiological data collected by the sensor networks can be stored for a long period of time, and can be used for medical exploration. The installed sensor networks can also monitor and detect elderly people's behavior, e.g., a fall. These small sensor nodes allow the subject a greater freedom of movement and allow doctors to identify pre-defined symptoms earlier. Also, they facilitate a higher quality of life for the subjects compared to the treatment centers.

Tracking and monitoring doctors and patients inside a hospital: Each patient has small and light weight 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.

1.2.4 Home Applications

Home automation: As technology advances, smart sensor nodes and actuators can be buried in appliances, such as vacuum cleaners, micro-wave ovens, refrigerators, and VCRs. These sensor nodes inside the domestic devices can interact with each other and with the external network via the Internet or Satellite. They allow end users to manage home devices locally and remotely more easily. Smart environment: The design of smart environment can have two different perspectives, i.e., human-centered and technology-centered. For human-centered, a smart environment has to adapt to the needs of the end users in terms of input/output capabilities. For technology-centered, new hardware technologies, networking solutions, and middleware services have to be developed. A scenario of how sensor nodes can be used to create a smart environment. The sensor nodes can be embedded into furniture and appliances, and they can communicate with each other and the room server. The room server can also communicate with other room servers to learn about the services they offered, e.g., printing, scanning, and faxing. These room servers and sensor nodes can be integrated with existing embedded devices to become self -organizing, self-regulated, and adaptive systems based on control theory models as described in.

II. WIRELESS SENSOR NETWORK ARCHITECTURE

There are basically two components in the infrastructure of a wireless sensor network: sink nodes and sensor nodes. But it is described by four parameter.

- **Sensor motes (Field devices)** – capable of routing packets on behalf of other devices.
- **Gateway or Access points** – A Gateway enables communication between Host application and field devices.

- **Network manager** – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.
- **Security manager** – The Security Manager is responsible for the generation, storage, and Management of keys.

2.1 Challenges in Wireless Sensor Network

There are various types of challenges wireless sensor network has to face also due to the nature of their work. Along with different type of attack by adversary, developing sensor networks that ensures high-security features with limited resources is a challenge too. WSN cannot be costly made as there is always a great chance that they will be deployed in different environments and captured for key information or simply destroyed by an adversary, which, in turn, can cause huge losses. Part of these cost limitation constraints includes an inability to make sensor networks totally tamper-proof. Other sensor node constraints that must be kept in mind while developing a key establishment technique include battery life, transmission range, memory, and deployment knowledge. The challenges are discussed details in the following sections.

2.1.1 Lifetime

One of the most important challenges in wireless sensor networks is to increase the lifetime of the entire network. Sensor nodes will sense a physical phenomenon, perform processing operations on detected events, store data, and transmit observations to a central point. These actions obviously consume power resources, thereby making power consumption a primary consideration. For instance, the Mica mote will exhaust its entire power supply during the first two weeks of deployment if it continuously operates at full power. To increase node lifetime two years, it is essential to run the sensor node on a duty cycle of less than one percent. Besides, many experiments have shown that transmitting a single bit uses the same power resources as executing 800 to 1000 computational instructions. Under such circumstances, much research has been conducted to decrease the amount of energy used in data transmission and Communication. For example, the Medium Access Control (MAC) layer has been modified to minimize channel listening without increasing collisions and packet retransmissions. Moreover, the network layer has been modified to control the packet reception, packet forwarding, and routing table update exchanges. Thus, developing an efficient key management scheme requires the economical consumption of available power resources [14][15].

2.1.2 Fault Tolerance

Some sensor nodes may die due to unexpected troubles in their physical components such as a power supply shortage, obstacles in the terrain where they are deployed, the presence of noise, or the occurrence of jamming. As mentioned earlier, wireless sensor networks operate most of times in outdoor or perilous environments so that crucial events can be observed and detected within an acceptable response time. Because of this criticality, the area of interest should be covered with a satisfactory amount of nodes every moment even though a set of sensor nodes become unreachable for whatever reason. In other words, any failure of a sensor node must encourage the network to adapt itself with sudden changes in topology, thereby not affecting the performance and connectivity of the entire network.

2.1.3 Maintenance

As we know, replacing or recharging the power supplies of sensor nodes as well as repairing computation and transmission units is not possible in wireless sensor networks. Therefore, protocols must be designed to optimize use of available hardware in order to increase the lifetime of the network. On the other hand, the nature of sensor networks requires software maintenance. For example, sensor nodes perform their tasks with the aid of a tiny operating system and a set of predefined programs. In the case when an administrator adds or removes a certain sensor node task, they have to change or update the programs running on the nodes by redistributing new software. In this scenario, wireless sensor networks should prevent the loss of update packets and authenticate the identity of the originators. Furthermore, sensor nodes should be able to self-configure themselves with the latest tasks. Another maintenance function is network synchronization since timing plays an important role in many network operations such as data aggregation and key management.

2.1.4 Scalability

Many wireless sensor networks take advantages of an enormous number of sensor nodes so that observation objectives are achieved. After the deployment phase, it is also possible to find situations where supplementary nodes are deployed in a random manner to improve network performance. As a consequence, protocols in wireless sensor networks must be designed with an ability to work in environments in which the number of sensor nodes is large. A further challenge for sensor network protocols is the region density, that is, the number of sensor nodes in a specific area. As a matter of fact, the density of a region will have a significant impact on various protocols and techniques. To illustrate, exploiting flooding mechanisms to broadcast certain information in a network whose density is low can be an economic option, but it will consume a lot of resources in sensor networks with high density regions.

2.1.5 Attacks

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Here we discusses different types of attacks in wireless sensor networks in next chapter

2.1.6 Battery life

Sensor nodes have a limited battery life, which can make using asymmetric key techniques, like public key cryptography, impractical as they use much more energy for their integral complex mathematical calculations. This constraint is mitigated by making use of more efficient symmetric techniques that involve fewer computational procedures and require less energy to function [7].

2.1.7 Transmission range

Limited energy supply also restricts transmission range. Sensor nodes can only transmit messages up to specified short distances since increasing the range may lead to power drain. Techniques like in-network processing can help to achieve better performance by aggregating and transmitting only processed information by only a few nodes. This way it can save the dissipated energy[7][8].

2.1.8 Memory

Memory availability of sensor nodes is usually 6–8 Kbps, half of which is occupied by a typical sensor network operating system, like Tiny OS. Key establishment techniques must use the remaining limited storage space efficiently by storing keys in memory, buffering stored messages, etc[9][10].

III. REQUIREMENTS, CONSTRAINTS AND EVALUATION METRICS OF WSN

Before going into detailed discussion about individual scheme we would like to discuss about the characteristics of secure communication in wireless sensor network. The achievement of communication security is a challenging task because of the "fragile nature" of WSN. WSN have a set of characteristics which complicates the implementation of traditional security and key management solutions. First of all, the wireless nature of communications in WSN makes it easier for attackers to intercept all transmitted packets. Second, WSN are constrained by the limited resources. Due to the following limitations, it is difficult to implement complicated security solutions in WSN. Third, in many cases, a large number of sensors are needed to be deployed in a hostile environment, which makes it very hard to have a continuous control on sensors. Finally, WSN are vulnerable to physical attackers. An attacker can capture one or more sensors and reveal all stored security information (particularly stored keys) which enables him to compromise a part of the WSN communications. For all these reasons, an efficient key management scheme should be implemented in the sensor before its deployment. The key establishment technique employed in a given sensor network should meet several requirements to be efficient. These requirements may include supporting in-network processing and facilitating self-organization of data, among others. However, the key establishment technique for a secure application must minimally incorporate authenticity, confidentiality, integrity, scalability, and flexibility sensor network has some exclusive requirements:

Data Authentication: Data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data [13].

Data Confidentiality: In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure Communication channel in a wireless sensor network. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet.

Data Freshness: Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design[14][15].

Self-Organization: A wireless sensor network is a typically an ad hoc net- work, which requires every sensor node be independent and flexible enough to be self organizing and self-healing according to different situations.

Time Synchronization: sensors may wish to compute the end-to end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc.

Integrity: Here integrity means only the nodes in the network should have access to the key sand only an assigned base station should have the privilege to change the keys. Unauthorized nodes should not be able to establish communications with network nodes and thus gain entry into the network.

Scalability: Sensor networks should employ a scalable key establishment technique. Key establishment techniques employed should provide high-security features for small networks, but also maintain these characteristics when applied to larger ones.

Flexibility: Key establishment techniques should be able to function well in any kind of environments and support dynamic deployment of nodes, i.e., a key establishment technique should be useful in multiple applications and allow for adding nodes at any time. A key establishment technique is not judged solely based upon its ability to provide secrecy of transferred messages, but must also meet certain other criteria for efficiency in light of vulnerability to adversaries, including resistance, revocation, and resilience.

Resistance against node capture: An adversary might attack the network by compromising a few nodes in the network and then replicate those nodes back into the network. Using this attack the adversary can populate the whole network with his replicated nodes and thereby gain control of the entire network. A good key establishment technique must resist node replication to guard against such attacks.

IV. CONCLUSION AND FUTURE WORK

We studied the problem of sensor localization in the presence of malicious adversaries and proposed a high-resolution range-independent localization scheme called HiRLoc. We showed that HiRLoc localizes sensors with significantly higher accuracy than previously proposed methods, while requiring fewer hardware resources. Furthermore, we showed that HiRLoc allows the robust location computation even in the presence of security threats in WSN, such as the wormhole attack, the Sybil attack and compromise of network entities. Our simulation studies confirmed that variation of the transmission parameters at the reference points leads to high-resolution location estimation.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” Computer Networks, vol. 38, no. 4, pp. 393-422, 2009.

[2] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, “Wirelesssensor networks for habitat monitoring,” in Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, pp. 88-97, 2008.

[3] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, “System architecture directions for networked sensors,” SIGOPS Operating System Review,vol. 34, no. 5, pp. 93–104, 2010.

[4] D. Puccinelli and M. Haenggi, “Wireless sensor networks: Applications and challenges of ubiquitous sensing,” IEEE Circuits and Systems Magazine, vol. 5, no. 3,pp. 19-29, third quarter 2009.

[5] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” Ad Hoc Networks, vol. 1, no.2-3, pp. 293-315, September 2011.

[6] G. Hoblos, M. Staroswiecki, and A. Aitouche, “Optimal design of fault tolerant sensor networks,” in Proceedings of IEEE International Conference on Control Applications, Anchorage, AK, September 2008, pp. 467–472.

[7] J. Bachrach, C. Taylor. “Localization in sensor networks Handbook of Sensor Networks: Algorithms and Architectures”, Hoboken: John Wiley & Sons, 2009, pp. 277 – 310.

[8] G. Mao, B. Fidan, B. D. Anderson. "Wireless sensor network localization techniques. Computer Networs", 2010, 51(10), pp. 2529– 2553.

[9] Adel Youssef and Moustafa Youssef. A Taxonomy of Localization Schemes for Wireless Sensor Networks. In ICWN, pages 444-450, 2009.

[10] E. Sabbah and K-D Kang, "Security in wireless sensor networks," in Guide to Wireless Sensor Networks, London: Springer-Verlag, page:511-512, 2009.

[11] "ROPE: robust position estimation in wireless sensor networks," in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, April 2011, pp. 324–331.

[12] L. Lazos and R. Poovendran, "SeRLoc: Secure range independent localization for wireless sensor networks," in Proceedings of the 3rd ACM Workshop on Wireless Security, 2011

[13] L. Lazos and R. Poovendran, SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks, to appear in Proceedings of WISE, Philadelphia, PA, Oct. 2004, pp. 21–30.

[14] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In Proceedings of IEEE INFOCOM '05, 2005.

[15] F. Anjum, S. Pandey, P. Agrawal. Secure localization in sensor networks using transmission range variation. 2nd IEEE International Conference on Mobile Adhoc and Sensor Systems, MASS '05, pp. 195-203, November 2005.