ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Detection of course-plotting Protocols in Wireless Sensor Network security

PRIANKA.R.R[1], BIBIN.M.R[2]

1. Assistant Professor, RMK College of Engineering and Technology Puduvoyal ,Chennai- 601206

2. Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering Colleg,Avadi

Manuscript Info

Manuscript History:

Received: 15 October 2015
Final Accepted: 26 November 2015
Published Online: December 2015

Key words:

Wireless sensor networks; Attacks; Intrusion detection; Authentication; Transmission.

Corresponding Author

PRIANKA.R.R

Abstract

Wireless Sensor Networks (WSNs), providing end to end secure interactions between sensors and the sink is important for secure network managing. In the great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. One of the major challenges wireless sensor networks face today is security. The sensing technology combined with dealing out power and wireless communication makes it lucrative for being exploited in great extent in future. The wireless communication technology also acquires various types of safekeeping threats and issues.

INTRODUCTION

A computing competence becomes rapidly growing smaller and cheaper with each passing year. The inexpensive, low-power communication devices can be deployed throughout a physical space, providing dense sensing close to physical phenomena, processing and communicating this information, and coordinating actions with other nodes. Combining these capabilities with the system software technology that forms the Internet makes it possible to implement the world with increasing fidelity.

To grasp this opportunity, information technology must address a new collection of challenges. The individual devices in a wireless sensor network (WSN) are inherently resource constrained. They have limited processing speed, storage capacity, and communication bandwidth. These devices have substantial processing capability in the aggregate, but not individually, so we must combine their many vantage points on the physical phenomena within the network itself.

Wireless communication and instrumentation have long been associated with remote sensing from satellites and missile telemetry—prime examples of wireless links. A network consists of many nodes, each with multiple links connecting to other nodes. Information moves hop by hop along a route from the point of production to the point of use. In a wired network like the Internet, each router connects to a specific set of other routers, forming a routing graph. In WSNs, each node has a radio that provides a set of communication links to nearby nodes. By exchanging information, nodes can discover their neighbours and perform a distributed algorithm to determine how to route data according to the application's needs.

The networking capability of WSNs is built up in layers. The lowest layer controls the physical radio device. Radios are by nature a broadcast medium: When one node transmits, a collection of others can receive the signal unless it is garbled by other transmissions at the same time. To avoid contending for the radio channel, the link layer listens on

the channel and transmits only when the channel is clear. It transmits a structured series of bits that form a packet encoded in the Radio signal. When not transmitting, nodes sample the channel and scan for a special symbol at the start of a packet that also lets the receiver align itself with the sender's time. The packet layer manages buffers, schedules packets onto the radio, detects or even corrects errors, handles packet losses, and dispatches packets to system or application components.

Sensor nodes are small in size, cheaper in price with restricted energy storage, less memory space and limited processing capability. Like all other wireless networks, remote wireless sensor networks are also vulnerable to many security threats. The unreliable communication and unattended installation of sensor nodes, increases difficulty in making the existing network security countermeasures efficient for these networks. The memory space and power restrictions of sensor nodes also make it difficult to implement traditional security solutions. So these networks require some unique security policies.

This paper describes Wireless sensor network architecture and characteristics in the section II overview of wireless sensor networks, attacks, security requirement, routing protocols and selective forwarding in section III and conclusion in section IV.

OVERVIEW OF WIRELESS SENSOR NETWORKS

Wireless sensor network architecture:

Two-tier architecture [1] consists of a set of nodes in place and a set of mobile nodes. Moving nodes form an overlay network or the role of data mules to transfer data across the network. In the three-tier architecture, a set of fixed sensor nodes transmit data at a set of mobile devices, which then transmits data to one set of access points. The heterogeneous network is designed to cover large areas and be compatible with several applications simultaneously. At the level of node, wireless sensors can be classified according to their role in the network.

Mobile embedded sensor:

The integrated mobile nodes do not control their own movement, but his movement is led by an external force, such as when connected to an animal, or connected to a shipping container.

Mobile actuated sensor:

Sensor nodes may also have the ability to motive power, which allows them to move in a sensitive region. With this type of controlled mobility, the implementation specification may be more accurate, the coverage can be optimized, and specific events can be targeted and controlled.

Data mule:

Often, the sensors should not be mobile, but you may need a mobile device to collect data and deliver them to a base station. These types of mobile entities are considered as mule's data. It is generally accepted that data mules can recharge their power sources automatically.

Access points:

In low density networks, or when you drop a node on the network, mobile nodes can be placed to maintain network connectivity.

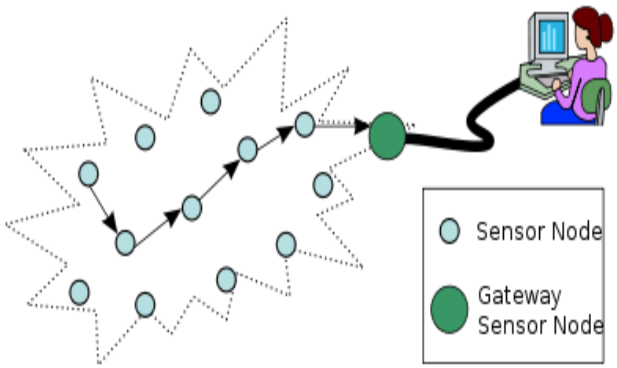

Fig.1 Two-tier architecture of WSN

The low cost small size sensors with more computational power are available in the market. Due to advances in technology the applications span over house hold usage to military. The sensitive applications demand secure transmission at the time of deployment of sensors. The applications include the following items. Cars, household items (microwave, refrigerator, washing machine), toys, and office equipment (doors, scanners, printers, and cameras)Control of heating, ventilation, detects the presence of biological and chemical presence.

Structural monitoring, tracking of shipment, global positioning system, health monitoring, shopping malls, building entries, remote control to televisions and motor vehicles. Traffic conditions, status of parking places, status of the hospital room conditions, and unauthorized entries in buildings.

The sensor applications in daily life includes from house related to military. Due to these reasons sensor research became very famous. The algorithms and protocols usage in networks and sensors is different due to nature of applications.

Some of the major differences between wireless sensor networks and wireless networks (ad-hoc networks) are:

Wireless sensor networks:
The wireless sensor nodes are densely deployed.
Topology changes frequently, since positions are not predetermined and nodes may fail at any time.
Limited memory, computational capability and transmission power. Global identification of a specific node may not exist. Sensor networks require special protocols to work with its design specifications.

Ad-hoc networks:
Deploying the nodes in ad-hoc are depends on the specific policy. Positions and policies are predetermined. Capabilities are differ from Wireless sensor networks. Each node is connected and identified. Traditional protocols use exchange and distribute the keys through cryptographic tools for trust evidence.

Characteristics of Wireless Sensor networks:
Non-centralized architecture: In WSNs, the status of every node is identical and no one is responsible for providing normal services. It is lack of a central administration and every node can join or disjoin the network any time. Besides, it does not affect the whole sensor network if some node failed and is reliable for applications with high stable requirement.

Self-organized:
The WSNs are characterized as Infrastructure-less networks and lack of fixed infrastructure. Thus, the sensor network is fully constructed by them when it is begin working with some pre-defined layering protocols and distributed algorithms. Once sensor networks are constructed completely, the sensor data would be collect and send to back-end system for further processing through the networks they built.

Multi-hop routing:
The sensor range of nodes in the WSNs is assumed to be limited, so if a node A would like to communicate with node D, which is out of communication range of node A. The node B would be a intermediate node and is responsible for transmitting the communication data to each other between node A and node B.

Dynamic topology:
In most of sensor network architecture assume that sensor nodes are deployed randomly and the network topology would be changed dynamically since the sensor node might be shut down, crash, recovery or utilize mobile sensors. 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. In Figure 2, two general organizations for distributed and hierarchical WSNs are illustrated.

A distributed/hierarchical structure of WSN consists of three types of participants, namely, a powerful back-end data centre, manager nodes and sensor nodes. Each manager node is responsible for collecting and forwarding all sensed

data of its managed area to the back-end data centre for further processing from sensor nodes under the area for which it is responsible.

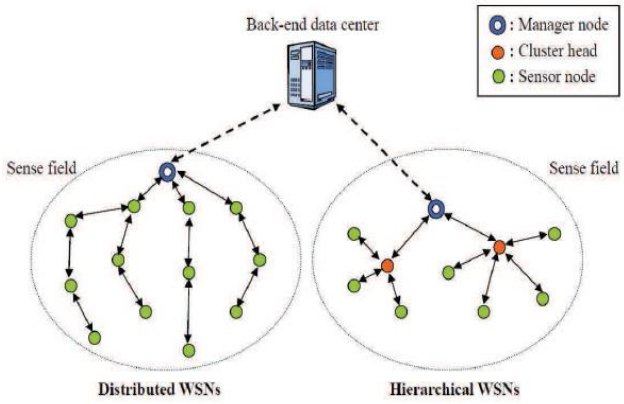

Fig 2: WSN organization

In distributed WSNs, a number of sensors are uniformly distributed into sense field and there are no specific roles for each deployment sensor node. In hierarchical WSNs, there are two types of roles for deployment sensors, namely: cluster head and sensor node. Based on geographical and deployment knowledge, a manager node groups all sensors into multiple logical groups and the grouping function is conducted through the selection of cluster head for each group. The main objective of cluster heads are acting as aggregation nodes and fusing the sense data collected from their nearby sensor nodes before routing the resultant data to a manager node. Therefore, cluster heads are much more computational and communication ability than normal sensor nodes in hierarchical WSNs.

Nodes are grouped into clusters with a cluster head that has the responsibility of routing from the cluster to the other cluster heads or base stations. Data travel from a lower clustered layer to a higher one. Although, it hops from one node to another, but as it hops from one layer to another it covers larger distances. This moves the data faster to the base station. Clustering provides inherent optimization capabilities at the cluster heads.

Mobility-based Protocols:
Mobility brings new challenges to routing protocols in WSNs. Sink mobility requires energy efficient protocols to guarantee data delivery originated from source sensors toward mobile sinks.

Multipath-based Protocols:
Considering data transmission between source sensors and the sink, there are two routing paradigms: single-path routing and multipath routing. In single-path routing, each source sensor sends its data to the sink via the shortest path. In multipath routing, each source sensor finds the first k shortest paths to the sink and divides its load evenly among these paths.

Heterogeneity-based Protocols:
In heterogeneity sensor network architecture, there are two types of sensors namely line-powered sensors which have no energy constraint, and the battery-powered sensors having limited lifetime, and hence should use their available energy efficiently by minimizing their potential of data communication and computation.

Quality of service based Protocols:
In addition to Minimizing energy consumption, it is also important to consider quality of service (QoS) requirements in terms of delay, reliability, and fault tolerance in routing in WSNs.
Selective forwarding

Selective Forwarding Attack is one of the network layer attacks. In multi-hop WSN, the nodes send packets to the neighboring nodes thinking that they forward messages to destination faithfully. In Selective Forwarding attack, malicious nodes legitimately refuses some packets and drops them. A simple form of this attack is when a malicious node acts like a black hole and drops all the packets passing through it. However in such an attack, the nodes can detect the attack and can exclude attacker from routing. A more refined of this attack is when a malicious node selectively drops / forwards packets. This makes detection of the attack more complicated.

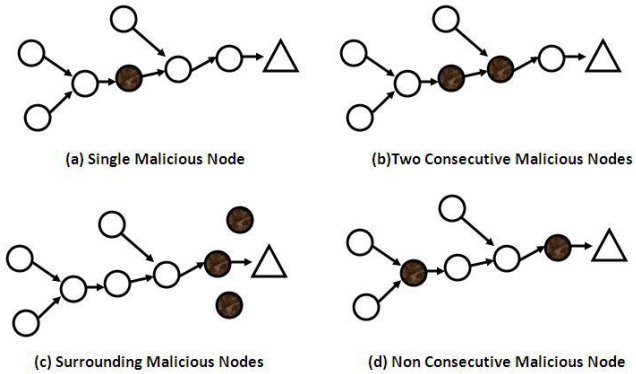

Fig. 3 Categorization of selective forwarding based on node count in Wireless sensor networks

Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow. However, it is conceivable an adversary overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest. In the Fig. 3 shown how many ways an adversary can deploy malicious nodes in transmission path to BS. Based on the packets it drops, selective forwarding can be classified into two types:
Drops packets of some specified nodes
Drops packets of some specified type
Evolution also generated attack strategy capable of dropping messages passing through his malicious nodes. This can be classified as a selective forwarding or black hole attack. Attacker found out several techniques for dropping messages.

The basic one is using simple DROP MESSAGE instruction from the set of elementary rules. But he was also able to find more complicated mechanism for dropping messages. He first stored the message into a memory slot, without its forwarding. Subsequently he overwrote the memory slot with another message. This approach is complicated and unnecessary indeed, but it demonstrates the capabilities of evolutionary algorithms to come up with several procedures to achieve the same goal.

Dropping messages occurred in strategies, whose evolution used the fitness functions based on number of delivered messages. This result was expected. However, it became also the basic principal of the strategies which tried to extend the path of the messages. This holds for both fitness functions including the length of path. Attacker tried to maximize the average length of the path by dropping messages which travelled only short distances.
To evolve these attack strategies, used three basic settings. First settings have fixed network topology and the message flows. Thus the attacker is able to make out messages witch travel only short distances by trying to drop them. Fitness value provides him with the feedback on how the average length has changed. In the next generation, attacker can try to drop another message.

The invader is thus learning the flows of data during the evolution. The ability of attacker to adapt the strategy for the concrete topology and traffic pattern can be classified as success. There can be applications with a priori known and fixed data flows and topology. In such scenario, attacker can optimize itself to achieve optimal results.

In the second setting used random topology and data flow for each attack strategy. This setting was not suitable for evolution. The fitness value achieved by an individual was highly dependent on the topology generated. Hence even poor individual was able to achieve good fitness value in the specific run of simulator. This led to varying fitness values and elimination of good Individuals.

A last setting uses the set of multiple different topologies and data flows for evaluation of a single attack strategy. We expected the downgrade of the fitness value, because evolution could not optimize the strategy for specific pattern. This probability was confirmed. However the evolution was still able to find at least some strategy for dropping the messages which improved its fitness value. These results have confirmed the predominating opinion, that evolution algorithms are primarily suitable for simple optimization problems.

Conclusions

The paper is all about implementation and detection of course-plotting protocols in wireless sensor networks. However, most of the security techniques rely heavily on a key allotment protocol and assume that top secret keys have already been placed on the distributed nodes. However as we showed, resourceful key distribution in WSN is no easy task.

As of now, still believe that there is much room for improvement in efficient key distribution in wireless sensor networks. As more efficient key distribution key mechanisms continue to appear, more efficient application specific security techniques will also emerge. But overall, perhaps the biggest challenge of all is proving that the proposed security techniques work well in real-world sensor network applications. All of this wireless sensor network research is producing a new technology which is already appearing in many practical applications.

References

[1] H. Karl and A. Willing, "Protocols and Architectures for Wireless Sensor Networks", John Wiley & Sons Ltd, 2005.

[2] T. Fujiwara, N. Iida, and T. Watanabe. An ad hoc routing protocol in hybrid wireless networks for emergency communications. In Proceedings of the 24th International Conference on Distributed Computing Systems Workshops—W6: WWAN (ICDCSW '04), pages 748–754, Tokyo, Japan, March 2004

[3] E. Shi and A. Perrig, "Designing Secure Sensor Networks," *Wireless Communication Mag.*, vol. 11, no. 6, Dec. 2004 pp. 38–43

[4] G. Xing, C. Lu, R. Pless, and Q. Huang, "On greedy geographic Routing algorithms in sensing-covered networks", *Proceedings ACM MobiHoc'04*, Tokyo, Japan, May 2004, pp. 31-42.

[5] S. Olariu, A. Wadaa, L. Wilson, and M. Eltoweissy. Wireless sensor networks: Leveraging the virtual infrastructure. IEEE Network, pages 51–56, July/August 2004.

[6] Healy.M, Newe.T, Lewis.E, „Security for Wireless Sensor Networks:A Review", IEEE Sensor Application Symposium, New Orleans, LA, USA-Feb 17-19, 2009.

[7] Yahaya.F.H, Yussoff.Y.M, Rahman.R.Ab, Abidin.N.H, "Performance Analysis of Wireless Sensor Network", 5th International Colloquium on Signal Processing & its Applications (CSPA), 2009.

[8] Rui Silva, Serafim Nunes "Security Issues on ZigBee" (2005), http://rtcm.inescn.pt/fileadmin/rtcm/WorkShop_22_Jul_05/s2_Security Issues_on_ZigBee.pdf. accessed: 5 January 2009.

[9] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Ad Hoc Networks, Vol. 1, No. 2, 2003, pp. 293-315.

[10] K. Sohrabi, J. Gao, V. Ailawadhi, and G. Pottie, "Protocols for selforganization of a wireless sensor network," *IEEE Personal Commu.*, vol. 7, no. 5, p. 1627, Oct. 2000.

[11] J. Hill, R. Szewczyk, A, Woo, S. Hollar, D. Culler, and K. Pister, System Architecture Directions for Networked Sensors, ASPLOS, November 2000.

[12] V. Giordano, F.L. Lewis, J. Mireles, B. Turchiano, "Coordination control policy for mobile sensor networks with shared heterogeneous resources," Proc. Int. Conf. Control & Automation, pp. 191-196, Budapest, June, 2005.

[13] Hung-Min Sun, Chien-Ming Chen, and Ying-Chu Hsiao. An Efficient Countermeasure to the selective forwarding attack in wireless sensor Networks.Pages1–4,Oct.2007.