ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
April 2014,
Vol. 7, No. (1):
Pgs. 75-81

Security Measures of WSN Networks by Avoiding Message Replay Attacks

GEETANJALI KANDHARI[1] and DEEPAK AGGARWAL[2]

[1]M Tech Student,BBSBEC,Fatehgarh Sahib
[2]Assistant Professor, BBSBEC,Fatehgarh Sahib

(Received: January 12, 2014; Accepted: January 20, 2014)

ABSTRACT

The challenges area of Ad Hoc networks is attributable to their lack of established infrastructure, requirement for redistributed management, dynamic topology, and wireless channel characteristics. We have a tendency to study the performance of IEEE 802.15 MAC protocol below varied conditions such as using Power control method and other techniques that improve better than of other Ad Hoc networks. To satisfy these needs a WSN networks is used to supports adaptively and improvement across layers of the protocol is needed. The WSN network improves better than other Ad Hoc networks types because in WSN the data only transferred when the both (sender /receiver) satisfied otherwise they kept on sleeping mode. The major challenge of this paper is to avoid the attacks because WSN continuously performed better than other technologies. The attack that is classified in the section 3; from these attack classification we analyze that the Message Replay attack is one of the more powerful attack that continuously touch with destination node and destination node assumes that the packets was received soon but an malicious node can't transferred the packets to the destination node. So in this stage message dropping start and the performance of the entire network goes down. We implement the secret key methodology in the network scenario so that each node communicates to other node only when if they having a secret key otherwise communication could not occurred. From the results studied it was observed that we improve the performances of WSN and avoided the Message replay attacks.

Key words:

INTRODUCTION

A wireless sensor network is a collection of nodes organized into a cooperative network. Wireless networks based upon IEEE 802.11 standards can now provide bandwidth approaching those of wired networks[4]. At the same time, the IEEE has noticed the low expense and high capabilities that sensor networks offer. The organization has defined the IEEE 802.15 standard for personal area networks (PANs), with "personal networks" defined to have a radius of 5 to 10 m. Networks of short-range sensors are the ideal technology to be employed in PANs. The IEEE encouragement of the development of technologies and algorithms for such short ranges ensures continued development of low-cost sensor nets.

Furthermore, increase in chip capacity and processor production capabilities has reduced the energy per bit requirement for both computing and communication. Sensing, computing, and communications can now be performed on a single chip, further reducing the cost and allowing deployment in ever larger numbers[4].In WSNs each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single Omni directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Such systems can revolutionize the way we live and work.

Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet[1]. This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces.

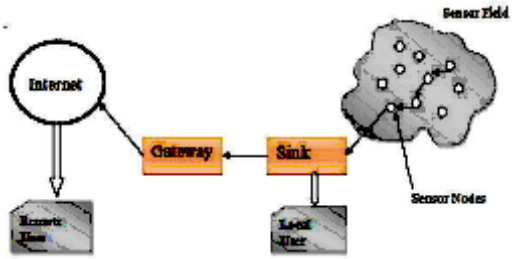

Fig. 1: Architecture of WSNs[2]

A wireless sensor network (WSN) in its simplest form can be defined as a network of (possibly low-size and low-complex) devices denoted as nodes that can sense the environment and communicate the information gathered from the monitored field through wireless links; the data is forwarded, possibly via multiple hops relaying, to a sink that can use it locally, or is connected to other networks (e.g., the Internet) through a gateway[2].

AODV Protocol

AODV is the simplest and widely used algorithm either for wired or wireless network. It is one of the most efficient routing protocols in terms of establishing the shortest path and lowest power consumption. It is mainly used for ad-hoc networks but also in wireless sensor networks. It uses the concepts of path discovery and maintenance [6]. However, AODV builds routes between nodes on-demand i.e. only as needed. So, AODVs' primary objectives are:

- To broadcast discovery packets only when necessary,
- To distinguish between local connectivity management (neighborhood detection)and general topology maintenance,
- To disseminate information about changes in local connectivity to those neighboring mobiles nodes that is likely to need the information.

AODV does not depend on network-wide periodic advertisements of identification messages to other nodes in the network. It periodically broadcasts "HELLO" messages to the neighboring nodes. It then uses these neighbors in routing.

Literature survey

John A. Stankovic, 2006 discussed the WSN issues and example solutions for the MAC layer, routing, localization, clock synchronization, and power management[1]. It described that how the solutions are different from past networking solutions. This discussion also provided a short description of two representative WSN systems: a military surveillance, tracking and classification system and an assisted living facility system. This study presents an overview of some of the key areas and research in wireless sensor networks. In presenting this work, examples of recent work are used to portray the state of art and show how these solutions were different from solutions found in other distributed systems.

Salvatore La Malfa, 2010 presented the definition of WSNs in real world[2]. The author

described the definition, the unique characteristics of wireless sensor networks and the characteristics of WSNs. It gives a brief description about the Sensor nodes architecture Operating systems and the introduction to IEEE 802.15.4, its various compatible platforms and the various applications of WSNs in real world.

Bhaskar Krishnamachari, 2005 this paper has given an overview of WSNs. It described that WSNs are a widely applicable, major emerging technology [3]. This paper brought a whole host of novel research challengespertaining to energy efficiency, robustness, scalability,self-configuration, etc. It described that challenges which are to be tackled at multiple levelsthrough different protocols and mechanisms. It also described that existing partial solutions offer much hope for the future,but much work remains to be done.

Chee-Yee Chong And Srikanta P. Kumar,2003

This paper traces the history of research in sensor networks over the past three decades, including two important programs of the Defense Advanced Research Projects Agency (DARPA) spanning this period: the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SensIT) programs [4].Technical challenges in sensor network development include network discovery, control and routing, collaborative signal and information processing, tasking and querying, and security. The paper is concluded by presenting some recent research results in sensor network algorithms, including localized algorithms and directed diffusion, distributed tracking in wireless ad hoc networks, and distributed classification using local agents.

Ed Callaway et. Al, 2002 this article presents the IEEE 802.15.4 draft standard and its home networking applications[5]. The main features of the standard are network flexibility, low cost, and low power consumption; the standard is suitable for many applications in the home requiring low-data-rate communications in an ad hoc self-organizing network.

Stephan Olariu, 2004 this paper described that Wireless sensor network research is an extremely challenging field. Lots of attention is needed while implementing WSNs[6]. This paper described that Wireless sensor Networks are far more vulnerable than wireless networks. Securing sensor networks is a subject of active work .This paper concluded that major challenge in WSNs is comprehensive information assurance in hybrid wired cum wireless networks.

WSN Attack Classification

Several attacks[8,9] thatare described below:-

Message Tampering Attack

An attacker can alter the content of routing messages and forward them with falsified information. By reducing the hop-count field in either an RREQ or RREP packet, an attacker can increase its chance to be an intermediate node of the route. A selfish node can relieve the burden of forwarding messages for others by setting the hop-count field of the RREQ to infinity.

Message Dropping Attack

Both attackers and selfish nodes can intentionally drop someor all routing and data messages. This attack can paralyze the network completely as the number of message dropping increases.

Message Replay (or wormhole) Attack

Attackers can retransmit eavesdropped messages again later in a different place. One type of replay attacks is the wormhole attack. A wormhole attacker can tunnel an RREQ directly to a destination node. Since a wormhole attacker may not increase the hop-count field value, it prevents any other routes from being discovered. The wormhole attack can be combined with the message dropping attack to prevent the destination node from receiving packets.

Eavesdrop on communication[9]

Process for intercepting packets flowing on the network.

Denial-of-Service (DoS)

After having supplanted as reliable nodes that contain valid routes to send packets, malicious nodes discard all messages received and not sent

to the destination node. This attack is also known as Black Hole Attack.

From the above attacks we are using Message replay attack for deploying on the network simulator and to avoid these attacks the following methodology adopted in the section 3.1.

Methodology Used

Collision avoidance is used to improve CSMA performance by not allowing wireless transmission of a node if another node is transmitting, thus reducing the probability of collision due to the use of a random truncated binary exponential back off time. The following Methodology used in this paper is:

Step 1 All nodes before entering the network procure a private key pair from CA and CA's private key.

Step 2 After that, nodes can generate a Group Session Key between immediate neighbors using a suitable 'Group keying protocol'.

Step 3 Secure AODV uses a central key management in its routing topology.

Step 4 These session keys are used for securing the routing process and data flow and hence the routing will be secure as well because only the source and destination will have the private keys at both end.

EXPERIMENTAL

In the Figure 2 showing that a packet moves from the source to destination along a chain of intermediate nodes. The successive packets sent by the source to a destination.

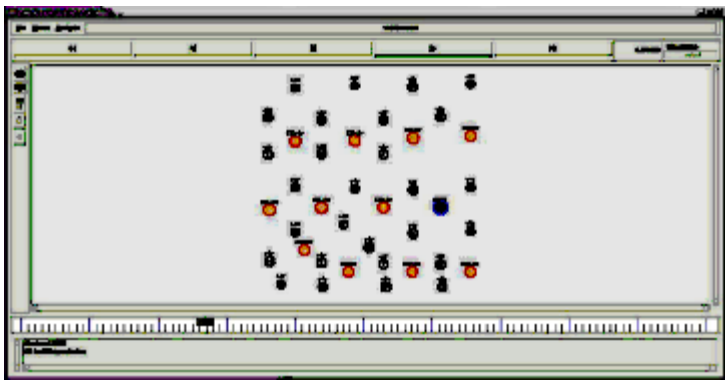

Fig. 2: Experiment Setup of WSN

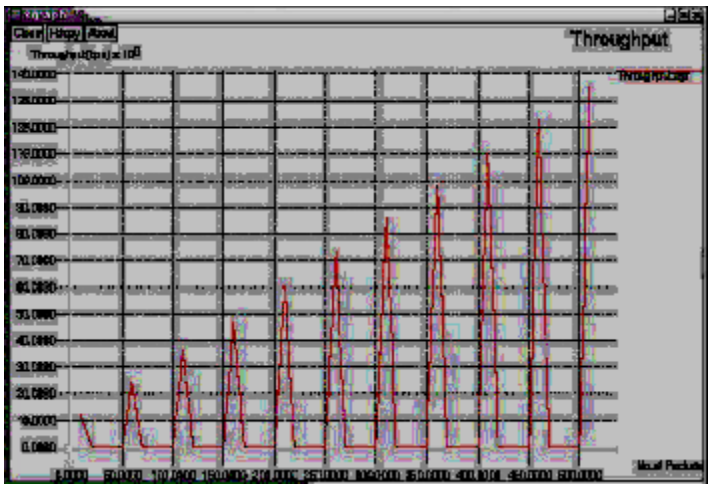

Fig. 3: Throughput of WSN (with message replay attack)

The blue circle is the sink node for communication range of a node, that is, it can communicate successfully with any node within this range. The orange circle is communicating nodes and black yet to communicate. In the black nodes in between the blue and red circles, the node is not able to communicate effectively but causes message replay.

RESULTS AND DISCUSSIONS

Throughput of WSN (with or after attack)

Throughput is defined as the number of bits of data successfully received at the destination per unit time. We investigate the impact of using different network topologies with varying number of interfering flows on achieved throughput and the effect packet size has on MAC layer performance by using three different packet sizes on each of the topologies.

From the achieved throughput in this case is 1.8 Mbps and with attack of message replay doesn't achieved the expected throughput and the data received with major delays and resultant attack by the malicious node on the network. On carefully observing the simulations above, we found two phenomena that result in degraded performance when offered message replay attack occurred shown in throughput (figure 3). The Figure 4 we rectify the attack attack by using the methodology represent in section 3.1.

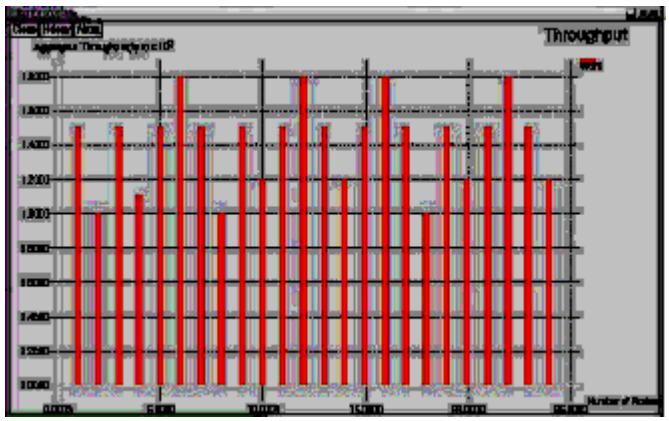

Fig. 4: Throughput of WSN (with rectify message replay attack)

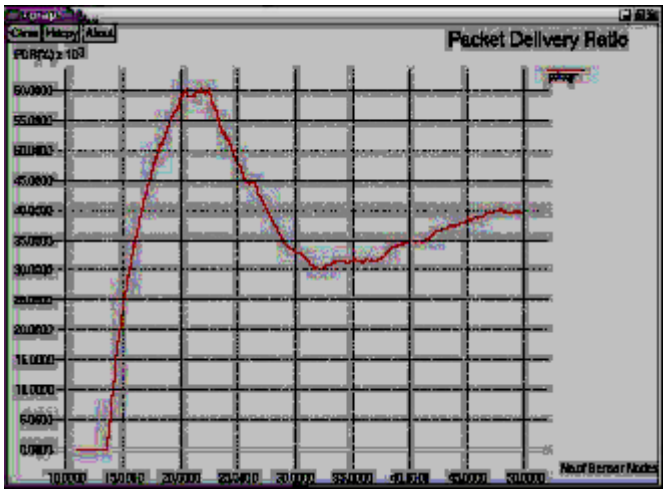

Fig. 5: Packet Delivery Ratio of WSN (with message replay attack)

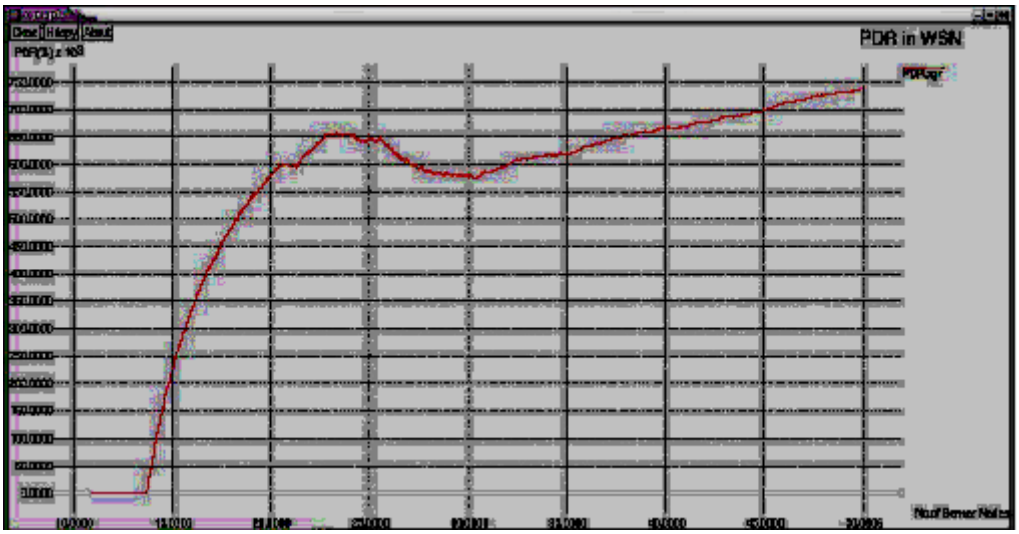

Fig. 6: Packet Delivery Ratio of WSN (with rectify message replay attack)

2 PDR (Packet Delivery Ratio) - with or after attack

The packet delivery refers to the successful delivery of packets from the sender to receiver side. If PDR50 percent than it means the attack happen on the network therefore possibly apply some security measures. From the figure 5 represents that the attack happens on the network area shown in the section 4. Therefore to apply the security (adapted methodology described in section 3.1) measures and hence PDR (figure 6) improves and resultant throughput is high (shown in figure 4) than throughput of WSN with message replay attack.

CONCLUSION

In this paper we apply the security measures in the wireless sensor networks to improve the performances of the network. The message replay attack harmful for wireless network so to rectify the attacks we used an methodology described in the section 3.1. We expect that gain the performances in respect of throughput and higher we have achieved.

Future Scope

This research of WSN security measures to handle message replay attack can be extended to more general complex topologies (added more attacks) and to handle with the above said methodology. Furthermore, the performance of WSN can also be studied under more general traffic patterns. That is traffic models that reflect real life patterns.

REFERENCES

1. John A. Stankovic, “Wireless Sensor Networks" (2006).
2. Salvatore La Malfa, “Wireless Sensor Networks " (2010).
3. Bhaskar Krishnamachari, “An Introduction toWireless Sensor Networks.” Tutorial Presented at the Second International Conference on Intelligent Sensing and Information Processing (ICISIP), Chennai, India, and January (2005).
4. Chee-Yee Chong and Srikanta P. Kumar,” Sensor Networks: Evolution, Opportunities and Challenges.” Proceedings ofthe IEEE, Vol. 91, No. 8, Pp. 1247-1256 (2003).
5. Ed Callaway, Paul Gorday, Lance Hester, Jose A. Gutierrez Marco Naeve, Bob Heile, Venkat Bahl, “Home Networking with IEEE 802.15.4: A Developing Standard for Low-

Rate Wireless Personal Area Networks." IEEE Communications Magazine, Pp.70-77 (2002).

6. Stephan Olariu, "Information assurance in wireless sensor networks." ODU Sensor Network Research Group (2004).
7. http://en.Wikipedia.Org/Wiki/Main_Page
8. Mohd Anuar Jaafar, Zuriati Ahmad Zukarnain, "Performance Comparisons Of AODV, Secure AODV And Adaptive Secure AODV Routing Protocols In Free Attack Simulation Environment", *European Journal of Scientific Research*, **32**(3): 430-443 (2009).
9. Carlos Felipe and Tellez Castano, "A Cryptography-Based Mechanism For Identifying Nodes Applied To Detection Of Wormhole Intrusion In Ad-Hoc Networks", (2012).
10. Madhav Sharma and Professor Rajeshwar Lal Dua , "Investigation Of Performance Metrics Of Dynamic Source Routing With Different Terrain Areas And Pause Time For Wireless Sensor Network", *International Journal of Advanced Research in Computer Science and Software Engineering Research Paper*, **2**(7): (2012).