QoS and Energy Consumption by Symmetric and Asymmetric key Schemes against Blackhole attack in Wireless Sensor Network

Er. Gurjot Singh
Computer Science and Engineering department
Baba Banda Singh Bahadur Engineering College,
Fatehgarh Sahib, Punjab, India

Er. Sandeep Kaur Dhanda,
Asstt. Prof.
Computer Science and Engineering department
Baba Banda Singh Bahadur Engineering College,
Fatehgarh Sahib, Punjab, India

Abstract— The Wireless Sensor Network consists of a number of spatial distributed sensor devices that combines with each other to accomplish a task of environment monitoring, object tracking, etc. and report the gathered data to a sink node through wireless interface. The unique properties of sensor networks such bounded power, stringent bandwidth, dynamic topology due to nodes failures, high network density and large scale deployments of sensor nodes have caused many critical challenges in the sensor networks. Due to this, the network is vulnerable to different severe attacks like blackhole attack that deplete the energy resources of the sensor nodes. These network demand energy awareness and robust security protocol designs at all layers of protocol stack. Energy consumption is an important issue in the design of wireless sensor networks which typically rely on non-renewable energy sources like batteries for power. Efficient utilization of sensor's energy resources and maximizing the network lifetime and the network security are still the main design considerations for the most proposed protocols for sensor networks. In this paper, the cryptographic based protocols i.e. IPSec and ANODR are implemented in wireless sensor network. These protocols provide security as well as quality of service to the sensor network. The performance of these protocols is analyzed on behalf of energy consumption in wireless sensor network.

Keywords- WSN, IPSec, ANODR, Energy, QoS

I. INTRODUCTION TO WIRELESS SENSOR NETWORK

In the recent years, the quick advancement in micro-electromechanical systems, low power, integrated digital electronics, bounded energy supply system, small micro-processors and low power radio technologies have created low power, low cost and multi-operational wireless sensor devices, which can observe the changes in physical phenomena of their surroundings. These sensor devices are equipped with a small battery, microprocessor, radio transceiver and a set of transducers that used to gather information and transmit it to base station that report the changes in the surrounding of the sensor node. The significance of these low cost and small size wireless sensor devices has motivated the research in data gathering and processing by combining some sensor devices, which led to the formation of Wireless Sensor Networks.

The WSN consists of a number of sensor devices that combines with each other to accomplish a task of environment monitoring, object tracking, etc. and report the gathered data to a sink node i.e. the base station through wireless interface.[1] However, with the unique properties of sensor networks such bounded power, stringent bandwidth, dynamic topology (due to nodes failures or physical mobility), high network density and large scale deployments of sensor nodes have caused many critical challenges in the design and management of sensor networks. These demand energy awareness and robust security protocol designs at all layers of the networking protocol stack [2].

Efficient utilization of sensor's energy resources and maximizing the network lifetime and the network security are still the main design considerations for the most proposed protocols and algorithms for sensor networks in this research area. However, limited energy is the most crucial one since in many cases it is impossible to replace or recharge batteries of the sensor nodes. Although energy harvesting via solar energy seems to be a promising solution to energy scarcity, present solar panels are still too large for tiny sensor devices. Eventually, proposed QoS support mechanisms must be lightweight and simple in order to operate on a highly

resource constrained sensor node [14]. In the different type of application, the gathered sensory data/ information normally have different attributes, where it may contain delay sensitive and reliability demanding information.

For the introduction of multimedia sensor networks along with the increasing interest in real time applications have made strict constraints on throughput and delay in order to report the time-critical data to the sink within certain time limits and bandwidth requirements without any loss of information. These performance metrics (i.e. Throughput, energy consumption, delay and bandwidth) are usually referred to as Quality of Service (QoS) requirements [3]. Therefore, enabling many applications in sensor networks requires energy and QoS awareness in different layers of the protocol stack in order to have efficient utilization of the network resources and effective access to sensors readings [4]. The node mobility, link failures due to unsecure wireless communication, node malfunctioning, energy depletion or natural causes like flood or fire results in topology changes. Moreover, most of the link layer or MAC layer protocols employ sleep-listen schedules and turn the radio of the sensor nodes off temporarily for energy saving. This kind of power management mechanisms also cause frequent topology changes. Inevitably, dynamic nature of the WSN topology introduces an extra challenge for QoS support [5].

II. SECURE ANONYMOUS ON-DEMAD ROUTING PROTOCOL

It is designed to provide a net-centric anonymous and untraceable routing scheme for wireless ad-hoc network. Anonymous On-demand Routing Protocol is designed to provide an anonymous and untraceable routing scheme for wireless ad-hoc networks. It is based on table-driven AODV routing protocol. As in other routing protocols network routes are open to all i.e. packets sent in wireless manner then any adversaries can trace the network route and infer the pattern of the packets that are being communicate between communicating parties. This may pose a serious threat to network [6]. It's a challenging constraint for routing and data forwarding. The ANODR protocol allows you to protect the wireless communication from being traced and without removing your devices battery. The adversaries should not trace the data packets that are sent by ANODR secure routing protocol. It provides untraceable path for data communication. The threats of being eavesdropped by others are less [6]. ANODR provides the following security services:

A. Negligibility- based on anti-tracing such that signal interceptors cannot trace signal transmitters mobility pattern via wireless signal tracing (with non-negligible probability defined on the victim network's size).

B. Confidentiality and anonymity- The path follows by the packets should not be traced by any adversaries.

C. Traffic flow confidentiality- Conceals the message content through encryption.

D. Identity-free routing- The identity cannot be stole by other.

E. One-time packet contents such that any two wireless transmissions are indistinguishable with each other in regard to a cryptanalyst.

The ANODR configuration is based on AODV parameter settings. ANODR parameters use the same terminology as AODV's parameters, except the name is changed from AODV to ANODR. These services are provided at the Network Layer and Link Layer to protect the IP and link layer protocols [12].

III. IPSEC PROTOCOL

IPSec is a standard suite of protocols prescribed by Internet Engineering Task Force (IETF), which provides data authentication, integrity, and confidentiality to data between communicating points across IP networks. It provides data/information security at the IP packet level and also provides end-to end security. It operates on the internet layer of the internet protocol suite [9]. IPSec works in two modes that are tunnel mode and transport mode. Transport Mode protects packets coming from transport layer to network layer by encapsulating the payload only but doesn't encapsulate the header. The IPSec header and trailer are added to message coming from transport layer. Transport mode is used when Host-to-Host protection of data is required. In tunnel mode full packet is protected along with the header. The IP header is added to the packet in this mode. Tunnel mode is used when communication held between two routers, a host and a router, or a router and host. There are two protocols in IPSec suite: Authentication header (AH) protocol and Encapsulating Security Payload (ESP) that provides authentication and encryption for packet security. Authentication header protocol authenticates the source host and ensures the payload integrity carried in IP packet. This protocol uses hash function and symmetric key to create the message digest; digest is inserted into authentication header and then AH is placed in appropriate place according to the mode. AH protects against unauthorized retransmission of packets by providing optional anti-replay protection. Authentication Header provides authentication and integrity, but doesn't provide privacy or confidentiality. If data is intercepted by intruders and only AH is used as security then the message contents can be read. For providing privacy or confidentiality Encapsulating Security payload (ESP) is used, which protect AH protects against unauthorized retransmission of packets by providing optional anti-replay protection against data tampering and most importantly provide message content protection. IPSec provides an open framework for implementing standard algorithms, such as MD5. These algorithms generate unique and unforgeable identifier for each packet, which is a data equivalent to a fingerprint. If some packets are tempered by intruder than this unique identifier helps in determining the tampered data. Along with Encryption/Decryption the ESP also performs

authentication that is called ESP authentication, using this ESP provides authentication and integrity for the payload and not for the IP header [6]. The authentication algorithms are compared separately for AH and ESP: with AH the MAC is calculated over the IP header and payload packet, while in ESP the IP header is neither encrypted nor authenticated [10, 11]. The computational and energetic demands introduced by cryptography, although significant, do not compromise the applicability of security solutions such as IPSec on sensor nodes. The new sensor nodes have more storage space than traditional devices i.e. sensor devices [11].

IV. BLACKHOLE ATTACK ON WSNS

A black hole attack is an attack that is mounted by an external adversary on a subset of the sensor nodes (SNs) in the network. The adversary captures these nodes and reprograms them so that they do not transmit any data packets, namely the packets they generate and the packets from other sensor nodes that they are supposed to forward. The malicious node starts advertising very attractive routes to data sink. The neighbor nodes of that malicious node select it as the next hop for forwarding the messages and considering it a high quality route. The neighboring nodes propagate this route to other nodes for communication. Thus all the network traffic get attracted to the malicious node that can either drop it, selectively forward it based on some malicious filtering mechanism or change the content of the messages before relaying it. This malicious node has thus formed a sink hole with itself at the center. The sink hole is characterized by intense resource contention among neighboring nodes of the malicious node for the bounded bandwidth, frequency and channel access [8]. This results in congestion and can accelerate the energy consumption of the nodes involved in the network that leads to the formation of routing holes due to nodes failure. With this several other types of denial of service attacks are then possible on the sensor network [7,8].

V. SIMULATION DETAILS

QualNet 4.5.1 Network Simulator tool is used to simulate and evaluate the cryptographic scheme against black-hole attack in wireless sensor networks. In the simulation scenario, the nodes are deployed randomly in a terrain of size of 1000*1000m. CBR is used as data traffic application with multiple source and destination. It consists of basic network entities as sensor nodes (mobile) and PAN coordinator. The PAN coordinator used is fully functioned and other remaining nodes are reduced function devices having limited constraints like storage, energy and power. The black-hole attack is implemented on random number of node in network. The security schemes IPsec is implemented on sensor network against black-hole attack. The performance is measured on the basis of energy consumption metrics. The simulation time is 200 second. For simulation the different parameters are set are shown in table 1:

TABLE 1. Simulation parameters setup for QualNet simulator

Terrain Size	1000*1000
Simulation Time	200sec
Radio/Physical Layer	802.15.4
Mac protocol	802.15.4
No. of Nodes	40
Secure Routing Protocol	ANODR
Attack	Blackhole attack
Security protocol	IPSec
Traffic Type	CBR traffic
Energy Model	Micaz
Mobility Model	Random Waypoint mobility
Device type	PAN coordinator, FFD and RFD

A. Simulation Scenario Design

The nodes are placed randomly on terrain of size 1000* 1000m. There are total 40 nodes placed on terrain. One wireless cloud is placed on the terrain has configured to 802.15.4. All the nodes are link wirelessly with the wireless subnet cloud except the two nodes. These nodes are link to another wireless subnet cloud that configure to blackhole attack. The nodes are made mobile nodes that move randomly on the terrain. CBR is used as data traffic application with multiple source and destination. Then IPSec protocol is configured on all the nodes and simulation is run for 200 seconds i.e the simulation time. The working of simulation is shown in figure 1.

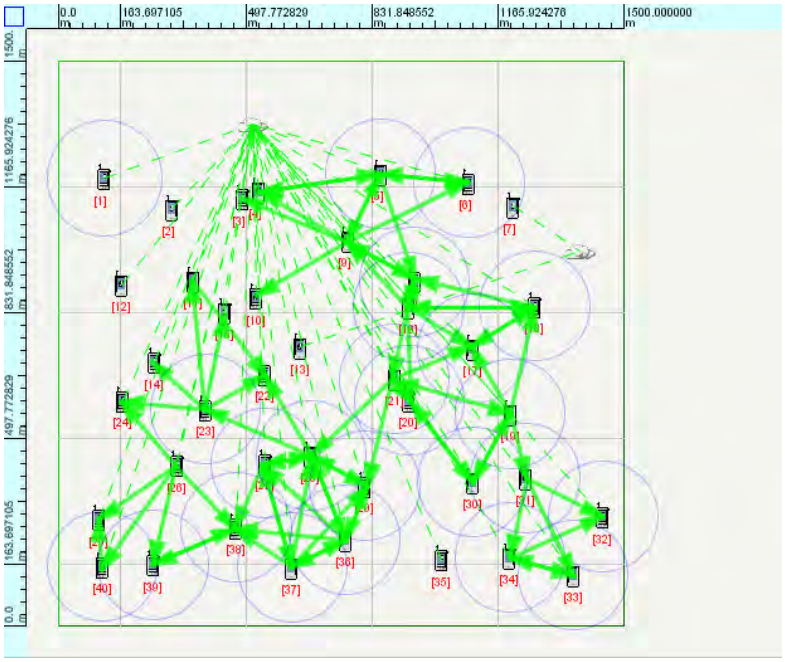

Figure 1. Working of Simulation Scenario

VI. RESULT AND DISCUSSION

In this section the energy consumed by symmetric and asymmetric key based cryptographic schemes are evaluated to prevent the blackhole attack in wireless sensor network. It has been analyzed on the basis of metric like energy consumed in transmit, received and idle mode of the network sensor nodes.

A. Energy consumed by IPSec and Anodr protocol in transmit mode at 40 nodes.

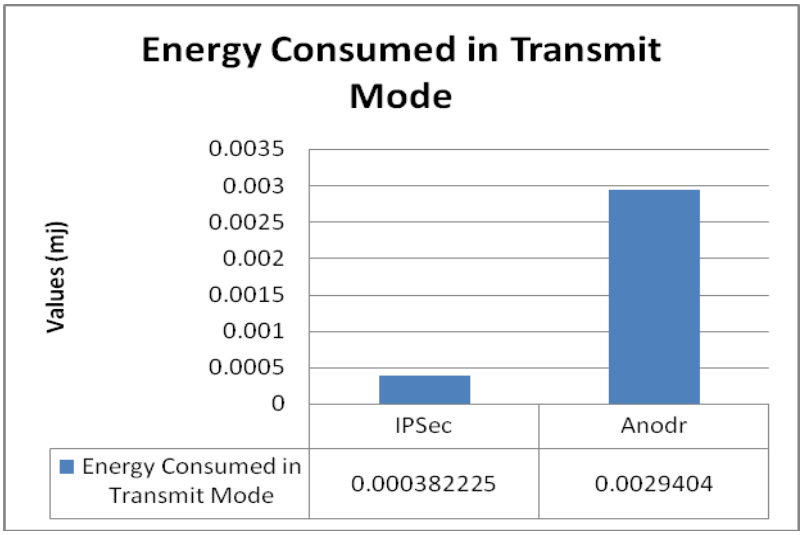

Figure2. Energy consumed in transmit mode

The above graph shows the energy consumed in transmit mode by Cryptographic schemes in wireless sensor network under blakhole attack. The value of energy consumed by symmetric key based scheme i.e. IPSec is 0.000382225 mj and by asymmetric key based scheme i.e. Anodr is 0.0029404 mj as shown in figure 2. The energy consumed by symmetric key scheme is less as compared to asymmetric key scheme as asymmetric key schemes require more storage space, computation power and more time for their processing.

B. Energy consumed by IPSec and Anodr protocol in received mode at 40 nodes.

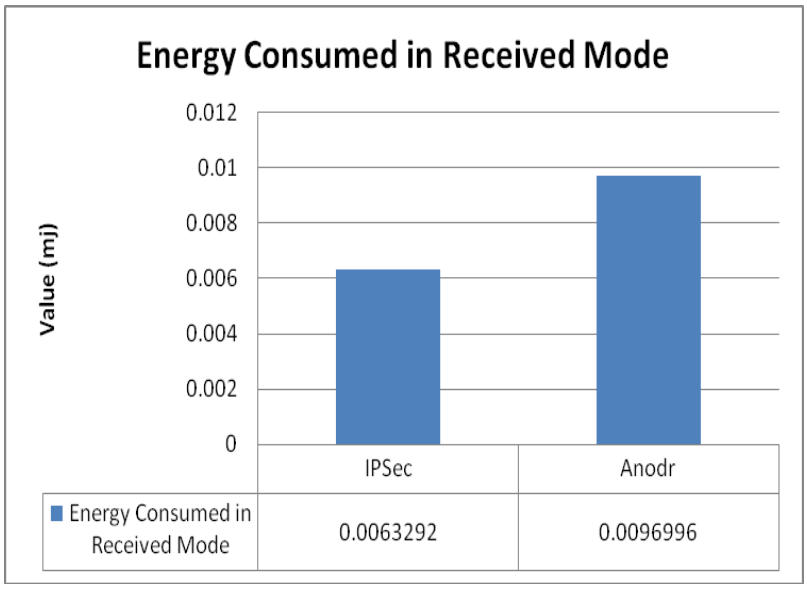

Figure 3. Energy consumed in receive mode

The above graph shows the energy consumed in received mode by Cryptographic schemes in wireless sensor network under blackhole attack. The value of energy consumed by symmetric key based scheme i.e. IPSec is 0.0063292 mj and by asymmetric key based scheme i.e. Anodr is 0.0096996 mj as shown in figure 3. The energy consumed in received mode by symmetric key scheme is less as compared to asymmetric key scheme.

C. Energy consumed by IPSec and Anodr protocol in idle mode at 40 nodes.

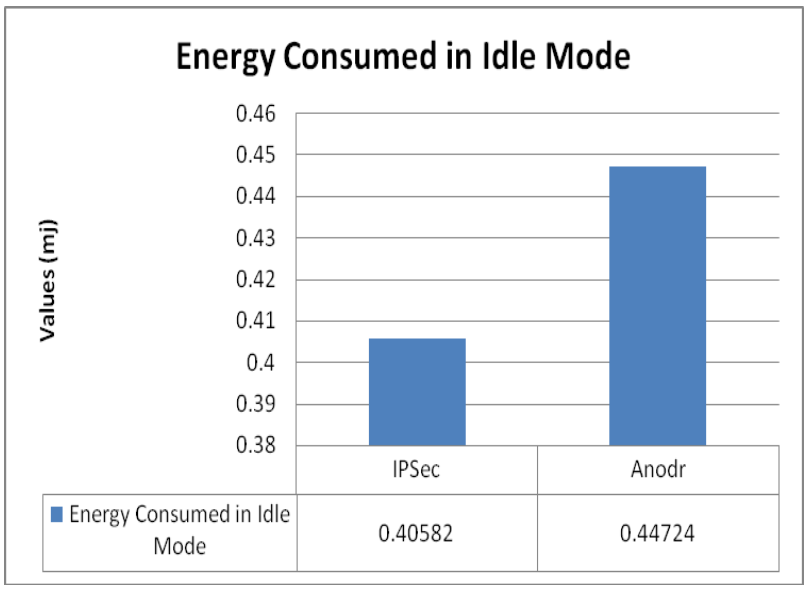

Figure 4. Energy consumed in idle mode

The above graph shows the energy consumed in idle mode by Cryptographic schemes in wireless sensor network under blakhole attack. The value of energy consumed by symmetric key based scheme i.e. IPSec is 0.40582 mj and by asymmetric key based scheme i.e. Anodr is 0.44724 mj as shown in figure 4. The energy consumed in idle mode by symmetric key scheme is less as compared to asymmetric key scheme.

VII. Conclusion

In this paper, the QoS and energy consumption by cryptographic key schemes under blackhole attack are evaluated. The IPSec scheme is based on symmetric key cryptography based schemes and it is considers as the main source of security and provide efficient QoS support in Wireless Sensor Network, till date. The selection of the appropriate cryptographic scheme depends on the processing capability of the sensor nodes characterized by the limited constraints such as its energy, computation capability, bounded memory and communication bandwidth. The mobility of sensor nodes has a great influence on the energy resources and security on sensor network topology. The IPSec symmetric key based scheme consumes less amount of energy in transmit, receive and idle mode as compared to asymmetric key based scheme i.e. ANODR protocol.

REFERENCES

[1] M. Hefeeda and M. Bagheri, "Wireless Sensor Networks for Early Detection of Forest Fires," The Proceedings of IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS-2007, Pisa, Italy, 8-11 October 2007, pp. 1-6.

[2] B. Yahya and J. Ben-Othman, "Towards a Classification of Energy Aware MAC Protocols for Wireless Sensor Networks," Journal of Wireless Communications and Mobile Computing, Vol. 9, No. 12, 2009, pp. 1572-1607.

[3] K. Akkaya and M. Younis, "A Survey on Routing for Wireless Sensor Networks," Journal of Ad Hoc Networks, Vol. 3, No. 3, pp. 325-349, 2005.

[4] Mohammad Reza Mazaheri, Behzad Homayounfar and Sayyed Majid Mazinani, " QoS Based and Energy Aware Multi-Path Hierarchical Routing Algorithm in WSNs", Scientific research-Wireless Sensor Network, 2012, 4, 31-39.

[5] M. Yigitel Aykut, Incel Ozlem Durmaz, Ersoy Cem, 2011, "QoS-aware MAC protocols for wireless sensor networks: A survey", Elsevier- Computer Networks, 55, pp. 1982- 2004.

[6] Gurjot Singh and Sandeep Kaur Dhanda, "Performance Analysis of Security Schemes in Wireless Sensor Network", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue. 8, pp. 3217- 3223, 2013.

[7] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In 1st IEEE International Workshop SNPA'03, May 2003.

[8] Anthony D. Wood and John A. Stankovic. Denial of service in sensor networks. IEEE Computer, 35(issue 10):48–56, Oct 2002.

[9] W. Znaidi, M. Minier and J. P. Babau, "An Ontology for Attacks in Wireless Sensor Networks" INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (INRIA), Oct 2008.

[10] Raza Shahid, Chung Tony, Duquennoy Simon, Yazar Dogan, Voigt Thiemo and Roedig Utz, 2011. "Securing Internet of Things with Lightweight IPsec", SICS, 2011, Vol. 8, pp. 1-26.

[11] Jorge Granjal, Ricardo Silva, Edmundo Monteiro, Jorge Sa Silva, Fernando Boavida, "Why is IPSec a viable option for Wireless Sensor Networks", IEEE, 2008.

[12] Er. Gurjot Singh, "Performance Analysis of ANODR and ZRP protocol against Wormhole attack in Wireless Sensor Network", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2. Issue 11 Nov.2013 Page No. 3346-3351.