RANGE BASED SEGMENTATION FOR WORMHOLE DETECTION IN WSN

Archna[1], Sukhjinder Kaur[2]

[1] Research Scholar, Sri Sukhmani College of Engg & Technology, Derabassi,
[2] Assistant Professor, Department of Electronics & Communication, Sri Sukhmani College of Engg & Technology, Derabassi,

ABSTRACT:

Modern wireless communication is very sensitive to various attacks due to less security while communication and less measure available for overcoming of protocols rules for communication. Wireless sensor network is type of network which is based on communication in ad-hoc manner. Wireless sensor network nodes sends data to a centralized node which act as sink and from sink it is used for graphical work and work based on various applications. Wireless sensor network is also prune to various attacks which could be available in ad-hoc communication. Wormhole attack is a common occurring attack which affects the wireless sensor network in term of data lost and more energy consumption. Protocols which are on demand in nature such as AODV (Ad-hoc On Demand Distance Vector) are very prune to wormhole attacks due to energy limitation and due to path finding technique which is very similar to the requirement of wormhole attack to launch. Wormhole attack is implemented in this paper for showing the effects of attack on the wireless sensor network protocol. With implementation of the wormhole attack, network throughput is low as compared to the normal network throughput. This comparison shows the dangerous effects of wormhole attack in AODV communication. Proposed mechanism is used to eliminate the attacker nodes from network. We have shown in simulation that wormhole attack affects the network in term of network performance degradation and recovery of the network performance.

KEYWORDS: Distributed Wormhole Attack, WSN-AODV, Wireless Sensor Network, On Demand Routing Protocols, Spoofing, Malicious Nodes.

INTRODUCTION

Wireless sensor networks are special segment of ad-hoc networks which are limited with energy for communication and mainly apply on remote areas to fetch various conditions. Data fetched by sensors collected in an aggregated manner and send the collected data to sink where sink processes it and send it to user defined applications. The basic structure of the wireless sensor network is defined in figure 1 below, which explains communication scenario between sensors and sink.

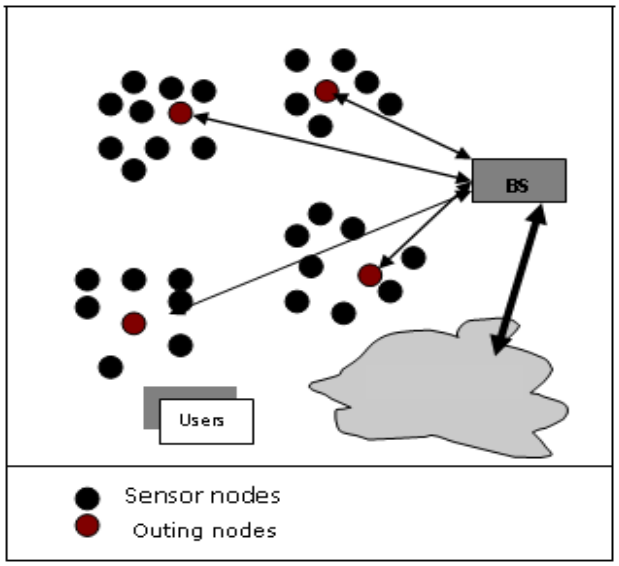

Figure 1: Communication scenario of sensor network with base station representing the sink [1]

Sensor network applied to various field to sense various types of conditions such as sensing temperature, climate conditions, water leveling, nuclear radiation detection, light detection, wind speed measuring etc. Different types of clustering approaches used in wireless sensor networks for saving the energy consumption for sensing the discussed situations. By applying these approaches, energy consumption is low as compared to communication with no clustering. All this affords are for saving resources of the network from sensor to sensor communication and sensor to sink communication. Every sensor hop is under limitation of energy and sensing capacity so sensors are distributed over the sensing field to fetch information.

Basic computation of the fetched dat is done by sensor and then it sends data to sink node for final processing of data.
Normally due to these processes in sensor network, sensors tends to save energy for longer communication but in case of any attack which consumes energy of the sensors and also halt the communication then sensor energy consumption rises and output comes to lower state.
Wormhole attack is a typical attack which could be easily launched in ad-hoc networks with very less affords so it is most occurred attack in ad-hoc communication network. Due to easy implementation this attack, sensors tends to lose energy and data and network performance goes low. Wormhole attack is very difficult to detect in sensor networks. Apart from energy consumption by wormhole attacker nodes, communication which is originally made by normal nodes is also halted by it. This attack is act more dangerous in case of sensor communication with omni-directional way as in this mode sensor network tends to send information faster as compared to passive communication in normal scenarios. Wormhole attackers also creates high speed tunnel which is used to send data fetched from network and use to send to other attacker at regular interval. Overall, wormhole attacker nodes halt the communication by implementing communication divergence to other attacker and normal communication lacks energy and communication of sensors under attack. In this paper, wireless sensor network is simulated and wormhole attack has been implemented in the network for fetching results and to find network performance.

REACTIVE PROTOCOL COMMUNICATI--ON IN WIRELESS SENSOR NETWORK

As we have discussed communication scenarios, protocol which drives the communication is very important part which decides the output of the network performance. In case of reactive protocol used in wireless sensor network, energy consumption is low so it is very useful to apply reactive protocols for communication.
Talking about the reactive protocol, AODV protocol comes into mind for its efficient and easy communication process. In most of the wireless sensor network setups, AODV is used due to its properties.
AODV is based on on-demand routing protocol which provide easy and better way of communication.
In AODV process, Hop count and delay on the route are the prime parameters to judge for selection of primary route for communication. If multiple route options from source to destination are available, then the route which provides less delay and less hop count will select as primary route for communication. Others route which having more delay and hop count is more are not considered for routing and these alternative routes are not stored in routing table. Due to this process, AODV provides quick convergence and less overhead.
Generally maintenance of AODV process is based on timely updates which suggest that entries into AODV process expired after timer expires [2] [3].
For basic selection of route, route request is use to broadcast to network and use to seek route reply messages from routes available on network. If no route reply received from any route then route error message will comes back to source node from where initial route request processed on first place.
With all advantages of AODV, there is a loophole which suits wormhole attack. Route discovery process of AODV protocol itself is providing suitable process for wormhole attack. In wormhole attack, attacker takes benefit of route discovery process of AODV, by introducing fake delay (provide less delay as compared to other alternative routes available originally for primary route to destination) and less hop count by pretending the attacker node as next hop node to destination which looks like least hop count to destination.

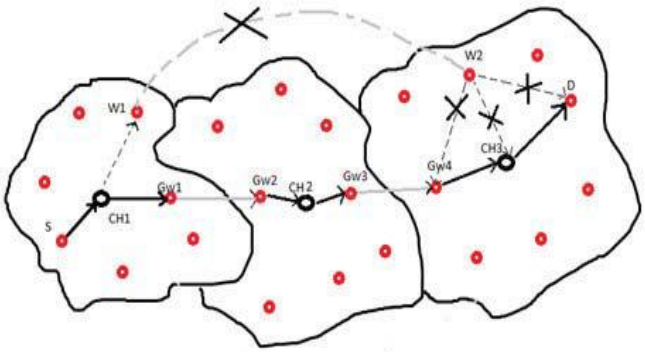

Figure 2: Wormhole Attack in Wireless Sensor Network [4]

During a wormhole attack, a malicious node copies data packets from one location in the network and tunnels them to another malicious node which is far away from source within the network, which replays them locally [4]. The logical link can be created and managed for long time in various ways, like an in-band and out-band channel which could be hidden. Packet processing is very fast as link established is very fast in processing with high powered transmission. Wormhole attackers nodes can transmit packets in inter cluster mode and intra cluster mode based on the tunnel speed established. Tunnel act as primary route, to source of the network so communication halt occurred in very structured manner without providing any

major upset in the network. Most of the prevention mechanisms are based on finding the attacker nodes by implementing algorithms which can track the variation and drop of packets on the next hop sensor node but most of the mechanisms are not able to avoid wormhole attack to be launched in AODV protocol communication.

EXPERIMENTATION

For experimentation purposes, OPNET simulation has been considered with implementation of wireless sensor network with equal amount of energy at initial stage. Some of the parameters used for experimentation are given in table 1 below:

Parameters	Value
Initial Energy	15 joules
Packet Exchange Speed	11 Mbps
No of Attackers	4
Protocol Used	AODV
Traffic Model	CBR
Pause Time	100 sec

Table 1: Parameters used for Experimentation

AODV protocol has been applied for routing purpose which provides fast and easy communication in sensor network.

Simulation is started with implementation of the routing process with 50 wireless sensor nodes in logical area. Traffic sent and Traffic received has been fetched for checking the performance of the network. After basic results of normal wireless sensor network, wormhole attackers have been introduced in the network and again traffic sent and traffic received have been fetched for the comparison of the results.

Various results fetched for basic communication and performance of AODV, Degradation in performance of AODV with effects of wormhole attack and Recovery of the network resources and performance of AODV with detection and elimination of wormhole attacks in term of throughput, delay, traffic receive and traffic sent in AODV network is discussed in the following sections.

VARIATION OF NETWORK PERFORMANCE IN TERM OF THROUGHPUT FOR PROPOSED WORK

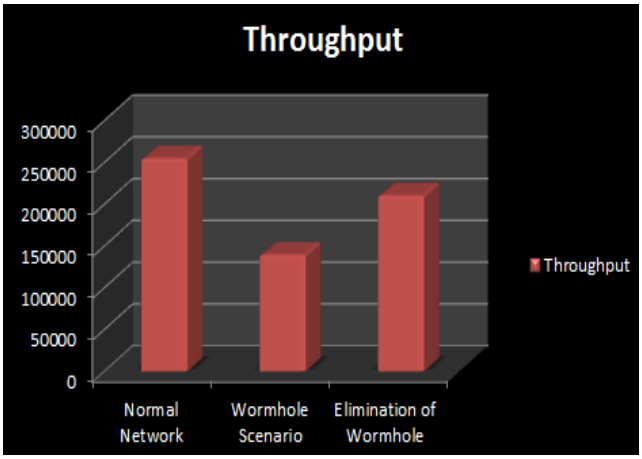

Figure 3: Throughput variance in case of normal, with attack and after elimination of attack

The performance of network is compared in above figure 3 and it is shown that basic communication of AODV network provide good level of throughput but performance decrease when applied under wormhole attack. Proposed work provides good recovery and throughput slowly tends to normal state throughput.

VARIATION OF NETWORK PERFORMANCE IN TERM OF DELAY FOR PROPOSED WORK

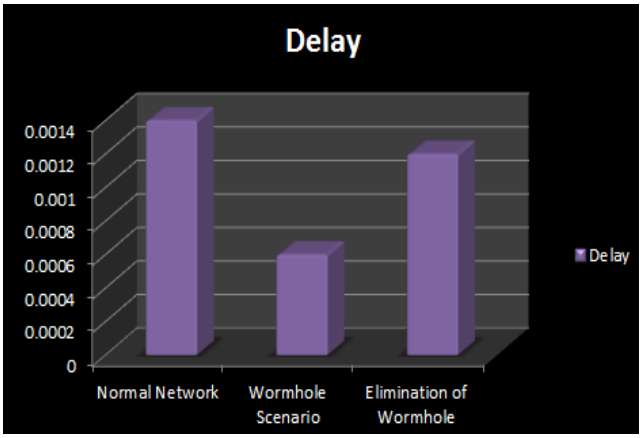

Figure 4: Delay variance in case of normal, with attack and with elimination of attack

The performance of network in term of delay is compared in above figure 4 and it is shown that basic delay in communication of AODV network provide normal level of delay but when network is affected by attack, delay is decreased which is shown due to effects of wormhole attack to fake the network credentials. Proposed work provides mechanism for delay management and delay slowly tends to normal state of delay.

Comparison of the fetched traffic sent and received is shown in below figures which provided us the idea of wormhole attack effects in the normal network.

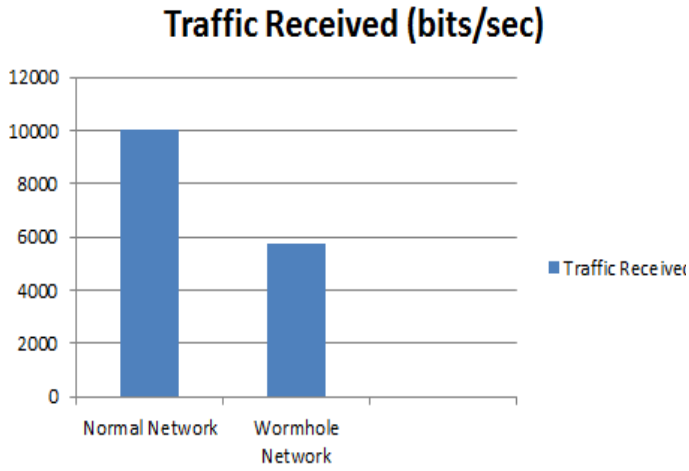

Figure 5: Traffic Received in term of bits/sec for Normal and Wormhole Scenario

Wormhole Network degrade the performance of the network as shown in figure 5, traffic received at the destination is very less in case of wormhole scenario which provides the sense of packet loss in wormhole scenario. The packets sent to other attacker not to the destination in network which is the reason of degradation of network performance. With more number of wormhole attackers, traffic received will be less and performance of the network will goes low and low once the wormhole attack is on peak. In prevention mechanism, traffic stabilization is the target.

The Normal network has provided better communication for wireless sensor network in case of traffic sent from source to destination. Comparison of the traffic sent for normal network and wormhole network is given below.

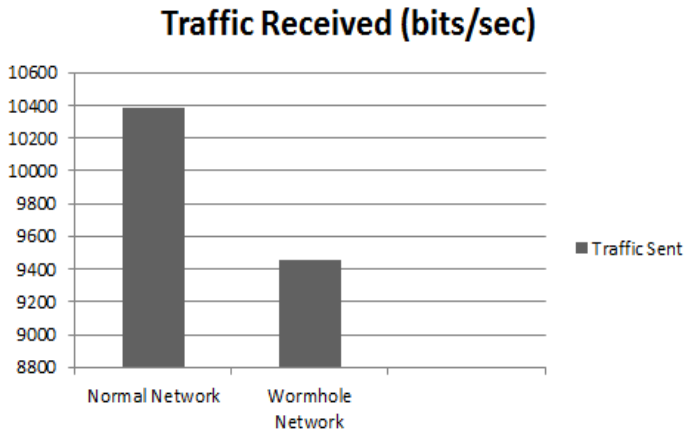

Figure 6: Traffic Sent in term of bits/sec for Normal and Wormhole Scenario

Traffic sent from source to destination is also low in wormhole network due to the tunnel processing in case of wormhole scenario. As come to normal sensor communication, wormhole provides less traffic sending which is a big issue which is needed to sort out in future.

CONCLUSION

In this work, the performance of the wireless sensor network with Ad-hoc on demand distance vector routing protocol has been summarized. The main focus was to show the performance of sensor network protocol AODV under normal environment, under wormhole attack and performance after elimination of wormhole attack in term of packet delivery ratio and overhead. In doing so, a wormhole scenario has been created and four wormhole attacker nodes have been generated. These malicious nodes provide false information to the network and AODV consider the path defined by malicious nodes as best routing path available and start communication through it. Performance of network decreases after wormhole attack and to eliminate of this attack, K-means clustering approach with header changes have been opted and implemented in network while communication. It maintains an average value for delay and number of hops. After implementation of this module, it finds the malicious nodes because the metric values of malicious nodes are very less as compare to normal metric value. A summary of suspected nodes has been forwarded to the upper layer where another module has been added to find the sequence of attack. If any sequence found, it is sent to network layer where another module is added to find the solution for attacks. Elimination of nodes takes place on Network layer by broadcasting the information of malicious nodes. Overall, elimination of wormhole attack has been done so that wireless sensor network communication can be normalized as normal communication.

REFERENCES

[1] Debnath Bhattacharyya, Tai-hoon Kim and Subhajit Pal,"A Comparative Study of Wireless Sensor Networks and Their Routing Protocols", International Journal of Sensor Communication, Vol.1, Issue.2, pp.34-38, November 2010.

[2] Mr. Susheel Kumar, Vishal Pahal, Sachin Garg, "Wormhole attack in Mobile Ad Hoc Networks: A Review" An International Journal on Engineering Science and Technology, Vol.2, No. 2, pp 65-69, April 2012.

[3] Routing protocols and concepts, CCNA exploration companion guide. ''Introduction to dynamic routing protocols''. Chapter three, pp 148-177.

[4] Amarjit Malhotra1, "Wormhole Attack Prevention using Clustering and Digital Signatures in Reactive Rou", IEEE International Journal of Innovation Technology, Vol.3, No.6, pp.84-89, June 2012.

[5] R.Vidhya, G. P. Ramesh Kumar, "Securing Data in Ad hoc Networks using Multipath routing", International Journal of Advances in Engineering & Technology, Vol.1, No. 5, pp 37-41, November 2011.

[6] Phuong Van Tran, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks", IEEE Conference on Consumer Communications and Networking, Vol.4, No.8, pp.93-98, January 2007.

[7] Turgay Korkmaz, "Verifying Physical Presence of Neighbors against Replay-based Attacks in Wireless Ad Hoc Networks", Information Technology: Coding and Computing, International Journal of Information Technology , Vol. 2, No. 2, pp 704-709, April 2005.

[8] Van Phuong T., Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, Heejo Lee, " Transmission Time-based Mechanism to Detect Wormhole Attacks", IEEE Conference on Asia-Pacific Service Computing Conference, pp 172- 178, December 2007.

[9] Ma Hongwei, "The Study on Ad hoc Networks Security Strategy based on Routing Protocols", IEEE International Conference on Computer Science and Network Technology, Vol.1, No.4, pp 445-449, December 2011.

[10] E.A.Mary Anita, V.Thulasi Bai, E.L.Kiran Raj, B.Prabhu, "Defending against Worm Hole Attacks in Multicast Routing Protocols for Mobile Ad hoc Networks" IEEE International Conference on Information Theory and Aerospace & Electronics Systems Technology, pp 1–5, March 2011.