Secure Routing Protocol in Wireless Sensor Networks for Vampire Attack

KEYWORDS

Sensor networks, security attacks, routing

L.LAKSHMANAN	Dr.D.C.Tomar
Research Scholar, Faculty of Computing, Sathyabama University, Chennai, India	Senior Professor, Department of IT,Jerusalem College of Engineering, Chennai, India

ABSTRACT *The vampire attack is a type of attack in which more energy is consumed by network than the original node during the transmission of message of same size to same destination. The vampire attack depends on the properties of routing protocols. Here we describe different methods to prevent the networks from vampire attack. The working environment is clearly tested in multi hop networks with inbound region and outbound regions. Hence the proposed model yields 78% in terms of secure data routing.*

I Introduction

A wireless ad hoc sensor network has a wide range of application in the communication environment. It is mostly used in the remote areas, in the military communication, for finding environmental disasters etc. The vampire attack consumes more energy from network than the original node during the transmission of message between nodes. Vampireattacks areof twotypes, one is carousel attack and the other one is stretch attack. In carousel attack the packets are send along a loop series where for many times the same node occurs in the route. In stretch attack the fake node will create artificially a long source path or routes, which results in the transmission of packets through a more number of nodes. It is difficult to prevent stretch attack.

A RELATED WORK

The Denial of service attacks results in eliminating the capacity of the networks to perform its functions. The jellyfish attack has an effect on the closed-loop, for example TCP and the black hole attack on the open-loop flows. In jellyfish attack the process of diagnosis and the detection of the malicious node are very costly and also consume more time, since it maintains compliance with the control and data plane protocols. Theblack hole and jellyfish attack has similar impact. The both jellyfish and black hole attacks are responsive to the condition of networks like loss and delay [1][2].

Daniel J.Bernstein and Peter Schwabe have proposed a new speed for AES software. In this paper the number of CPU instruction are reduced which are required for computation. It explain how many number of CPU cycle are reduced. The central idea of this paper lies in the study and grouping of these techniques, manufacturing remarkably high speeds for AES[4].

Tuomas Aura, PekkaNikander and JussipekkaLeiwo have proposed an authentication protocol in this paper of "DOS-resistant Authentication with Client Puzzles". In this paper the design principal is that the resources should be committed to the authentication protocol first and then it should be verified by the server. The Denial of service by the resource exhaustion is an important problem in open communication networks. The disadvantage is that other techniques are needed to protect separate clients against denial of services and to prevent exhaustion of communication bandwidth[3].

Gergely Acs, Levente Buttyan and Istvan Vajda has proposed a mathematical framework in which security is defined and routing protocols for mobile ad hoc protocols are analysed. A simulation based approach is followed to define and prove the security of ad hoc networks. Thus the usuage of proposed framework proved to be secure in the model but however some noteworthy features might inspire the designers of the future protocols.

In the existing system PLGP (Parno, Luk, Gaustad, and Perrig) and Destination Sequence Distance Vector (DSDV) are used[1][5]. The main disadvantage here is when the packets are transmitted from the source to the destination the data will be permanently stored in the nodes and each time it is retrived.A large amount of energy is wasted here for the storage and retrival process.

II PROPOSED METHODOLOGY

The proposed system includes Modified Destination Sequence Distance Vector(M-DSDV) protocol to prevent the draining of life from network nodes.In M-DSDV the data packets are temporarily stored in the nodes.When the packets are send to the neighbouring node, the data stored in it will be deleted.Each and every node knows the virtual address of the neighbouring node.

A NETWORK DESIGN

In M-DSDV the mobile nodes will form a group and will select a cluster head. The source node will send the data to the cluster headand the cluster head will forward it to the gateway node which is in the communication range of two or more cluster heads. The gateway node then forward the packets to the destination cluster head and the destination cluster head sends it to destination. In a dynamic network cluster head scheme can cause performance degradation due to frequent cluster-head elections, so MDSDV uses a Least Cluster Change (LCC) algorithm. In LCC, cluster-head change occurs only if a change in network causes two cluster-heads to come into one cluster or one of the nodes moves out of the range of all the cluster-heads. Fig.1, shows an example of CGSR routing scheme.

Each node maintains a cluster member table that has mapping from each node to its respective cluster-head. Each node broadcasts its cluster

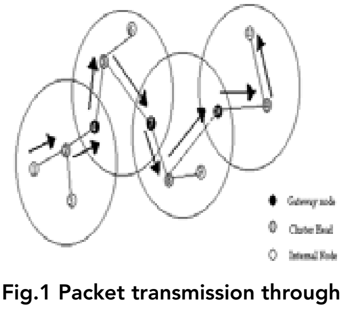

Fig.1 Packet transmission through gateway nodes.

Member table periodically and updates its table after receiving other nodes broadcasts using the M-DSDV algorithm. In addition, each node also maintains a routing table that determines the next hop to reach the destination cluster. On receiving a packet, a node finds the nearest cluster-head along the route to the destination according to the cluster member table and the routing table. Then it consults its routing table to find the next hop in order to reach the cluster-head selected in step one and transmits the packet to that node.

B ALGORITHM DESCRIPTION

The following steps are used in the M-DSDVprotocol.

Using the route discovery method the source node will find the path to the receiver node (sink). The source will send a request to send (RTS) message to the entire node.

When the sink receives the RTS it replies an acknowledgement to the source.

Then the source sends the data to the sink.

If any problem occurs the source won't get the acknowledgement in the given time period and the source will consider it as the path was failed.

The source will send the request to the cluster head.

The cluster head will receive the request from source and forward it to the failure detector. Using the passivemonitoring failure detector will then check the quality of the link.

Then the cluster head willimmediately selects the next possible path using the routing table which contains all the possible routes between the source and the sink.

III experimental approaches

A Network Topology

Each node sends "hello" message to other nodes which allows detecting it. Once a node detects "hello" message from another node (neighbour), it maintains a contact record to store information about the neighbour. Using multicast socket, all nodes are used to detect the neighbour nodes. The Cluster Head is elected based on Range, Battery and Mobility.

B PLGP Formation Tree Structure

Discovery begins with a time-limited period during which every node must announce its presence by broadcasting a certificate of identity, including its public key (from now on referred to as node ID), signed by a trusted offline authority. Each node starts as its own group of size one, with a virtual address 0. Nodes who overhear presence broadcasts form groups with their neighbours. When two individual nodes (each with an initial address 0) form a group of size two, one of them takes the address 0, and the other becomes 1. Groups merge preferentially with the smallest neighbouring group, which may be a single node.

C Secure Data Forwarding

During the forwarding phase, all decisions are made independently by each node. When receiving a packet, a node determines the next hop by finding the most significant bit of its address that differs from the message originator's address .Thus every forwarding event (except when a packet is moving within a group in order to reach a gateway node to proceed to the next group) shortens the logical distance to the destination, since node addresses should be strictly closer to the destination.

IV result and discussion

The Fig.2, shows the friction of total nodes/ friction of energy consumed during the implementation of plgp and M-dsdv. In M-dsdv initially the energy consumption will be higher since the nodes will take energy for the route discovery and the cluster head selection. Butgradually it decreases and will reach a moderate level.

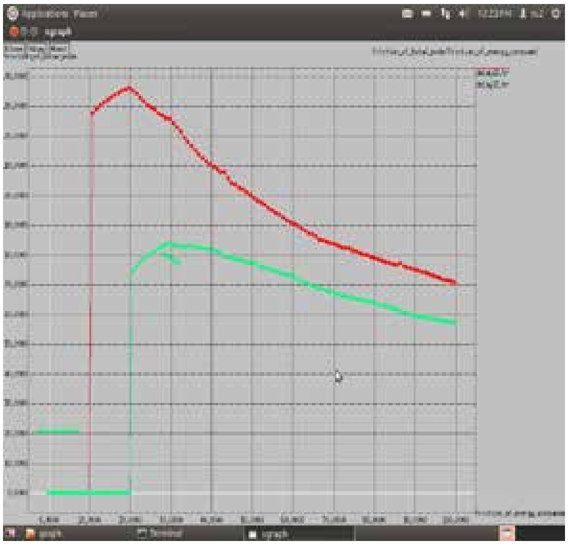

Fig.2 Energy consumption of PLGP and M-SDV

The Fig.3 shows the path length variation occurred during the plgp and M-dsdv implementation. The path length is comparatively less for M-dsdv when compared with the existing system.

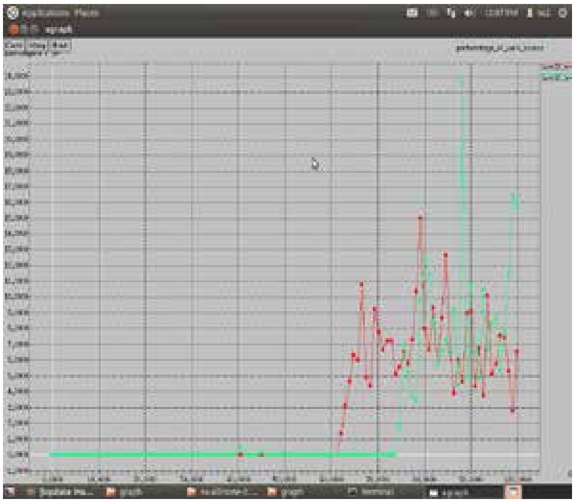

Fig.3 Path length of PLGP and M-DSDV

V Conclusion

Hence we conclude this paper with the appropriate result of secure routing, we have shown how the vampire attacks can be controlled or prevented by the implementation of Parno, Luk, Gaustad and Perrig [PLGP]and Modified Destination Sequence Distance Vector [M-DSDV]. The path length is comparatively less for M-DSDV when compared with the existing system. A high variation is shown for the existing system while the proposed one has slight one.

REFERENCE [1]Eugene Y.Vasserman and Nicholas Hopper, "Vampire attacks: draining life from wireless adhoc sensor networks, "IEEE Trans. Mobile Computing,vol. 12,no. 2,Feb 2013 | [2]G.Acs,L.Buttyan,and I.Vajda,"Provably Secure On-Demand Source Routing in Mobile Ad-hoc Network",IEEE Trans.Mobile Computing,vol.5,no. 11,pp.1533-1546, Nov.2006. | [3]T.Aura,"Dos-Resistant Authentication with Client Puzzles," Proc.Int'l Workshop Security Protocols,2011. | [4]D.Bernstein and P.Schwabe, "New AES Software Speed Records,"Proc.Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT),2008. | [5]B. Parno, A. Perrig, and V. Gliger, "Distributed Detection of Node Replication Attacks in Sensor Networks," in Proc. IEEE Symposium Security Privacy, 2005, PP. 49-63. | [6]Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based Compromise Tolerent Security Mechanism for Wireless Sensor Networks," in Proc. IEEE Symp. Security Privacy, 2005,PP.49-63. | [7]J.Deng, R.Han, and S.Mishra,"Defending against path-Based DoS Attack in Wireless Sensor Network,"Proc. ACM Workshop Security of ad hoc and Sensor Network,2005. | [8]J.Deng,R.Han,andMishra,"INSENS:"Instrusion-Tolerant Routing for Wireless Sensor networks," Computer and Comm,2006.,vol29,no.2,pp.216-230, | [9]I.Aad., J-P Hubaux and E.W Knightly, "Denial of Service Resilience in Ad hoc Network ", 2004. |