Dynamic Non-Linear Authenticator Protocol (DNAP) For MANETS

JayaPrakash .R[1], Saroja. K [2]

Research Scholar, Department of Computer Science, NASC, Erode, India[1]

Assistant Professor, Department of Computer Science, NASC, Erode, India[2]

Abstract: The Path Detection (PD) protocol used to select the shortest path and DNAP (Dynamic Non-linear authenticator Protocol) algorithm protocol used to find the alternate path to transfer a message to destination. To improve the detection accuracy to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, develop a dynamic Path routing protocol (DPR) mechanism based dynamic routing privacy preserving protocol architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes.

Keywords: Privacy preserving, Routing, Service, Authenticator.

I. INTRODUCTION

Wireless ad hoc networks have gained lots of attention due to their ease and low cost of deployment. This has made ad hoc networks of great importance in numerous military and civilian applications.

But, the lack of centralized management of these networks makes them vulnerable to a number of security attacks. One of the attacks is packet drop attack, where a compromised node drops packets maliciously.

II. APPLICATION AREAS OF WIRELESS SENSOR NETWORKS

a) Healthcare

Sensors are used in biomedical applications for healthcare. Sensors are implanted in the human body for monitoring medical problems such as cancer and help patients to maintain their health.

b) Building monitoring

Sensors can be used in buildings for detection of fire and smoke. In case of fire a network of sensors deployed in a huge building can track the source and direction in which fire is expanding. In addition, sensors can be used to monitor vibration that could damage the structure of a building.

c) Military

The use of WSN can provide real time information of the enemy activities to commando teams thus making coordination and planning more effective. The sensing, monitoring and decision-making should be integrated seamlessly, for designing effective military applications. The accurate and timely gathering of visual surveillance and intelligence data can play a central role in attaining objectives as well as minimizing loss of human lives.

III. EXISTING SYSTEM

A credit system provides an incentive for cooperation. A node receives credit by relaying packets for others, and uses its credit to send its own packets.A reputation system relies on neighbors to monitor and identify misbehaving nodes.The shape the traffic at the MAC layer of the source node according to a certain statistical distribution, so that intermediate nodes are able to estimate the rate of received traffic by sampling the packet arrival times.The Bloom filters to construct proofs for the forwarding of packets at each node. By examining the relayed packets at successive hops along a route, one can identify suspicious hops that exhibit high packet loss rates.

IV. DRAWBACKS IN EXISTING SYTEM

- As a credit system result, a maliciously node that continuous to drop packets will eventually deplete its credit, and will not be able to send its own traffic.
- A reputation node with a high packet dropping rate is given a bad reputation by its neighbors. This reputation information is propagated periodically throughout the network and is used as an important metric in selecting routes. Consequently, a malicious node will be excluded from any route.

V. PROPOSED SYSTEM

The methodology right from the network parameters as input until the link state routing protocol based on Dynamic routing algorithm measurement is explained as a step by step process below.

In wireless ad hoc networks, nodes communicate with each other using multi hop wireless links. Data to out of range nodes can be routed through intermediate nodes. That is nodes in wireless ad hoc networks can act as both hosts and routers. Network Model

DOI 10.17148/IJARCCE.2016.51015

a) Dynamic Non-linear authenticator Protocol

Dynamic Non-linear authenticator Protocol selects best routes based on the current state information for the network. The state information can be predicted or measured but the route will change depending on the available state information at the time of the traffic request. The privacy network can cope now with the dynamics of traffic and react to real-time network traffic accordingly, by introducing real-time behavior and state dependency in order to avoid congestion and to achieve optimal performance.

Dynamic routing protocol is distinguished by two factors:

- The computational model that the routing service is using
- The state information nature.

b) Algorithm for Dynamic Non-linear authenticator Protocol

- **Step 1** If the Source node S wants to send data to the destination node D, it will first send REQ message to all its neighbour nodes.
- **Step 2** When neighbour nodes receive REQ message they will check their broadcast, if this packet's ID is already in their Cache then packet will be discarded.
- **Step 3** Otherwise, node will calculate its energy by using: Enew = Etx - Er + Eth + Em + Eoverand send this value as a reply to source node.
- **Step 4** Source node will calculate the mean value of all the values of Enew of all the nodes and send a RREQ message to the node whose Enew value is nearest to the mean value.
- **Step 6** Assign the Attacker node depending on the routing environment.
- **Step 7** When the node receives a RREQ message it will send privacy preserving message to its own neighbors and this process will be continued till the destination node reaches.
- **Step 8** When destination node will receive the RREQ message it will send the RREP message back with the same route.

V. IMPLEMENTATION

The implementation for developing the dynamic privacy preserving measurement uses NS2.34 simulator. The protocol will provide a link state routing search in the network and prevent the packet drop in distributed manner.

Generally, LSR are categorized into two types: symmetrical and asymmetrical. The symmetrical LSRs are the cases where the distance (or cost) from starting point to end point is equal to the distance (cost). In this type of LSR, when number of nodes is given, there are always visible solutions. The task is to find which one of these solutions is the shortest in distance unit or least in cost unit. On the other hand, with the second type of LSR, the asymmetrical ones, the distance (cost) between two nodes differs by the direction. Thus, the distance (cost) from to is not equal to the distance. In this case, when number of nodes is given, there will be solutions. LSR usually assumes that the nodes can move freely from any directions, no matter which node the starting point .

VI. SIMULATION TIME CALCULATION

At this point, the simulation time can calculate its time by taking the last two points into account. Each tour time can be represented as

$$T_t = \left(\min_{dis} T / MA\_v\right) + (data/DR)$$

Where min_disis the minimum distance of the LSR, MA_vis the node velocity by the distance unit over the time unit, data is the collected data for each Routing Path (RP), and the DR is the data rate for each node.

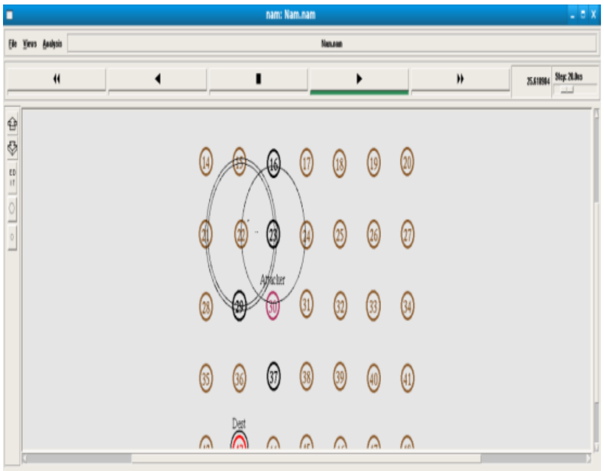

Fig.1 Choosing source and Designation

a) Attacker Generation process

Packet is moving from source to designation in between the user generating the attacker as any node in between the source to designation

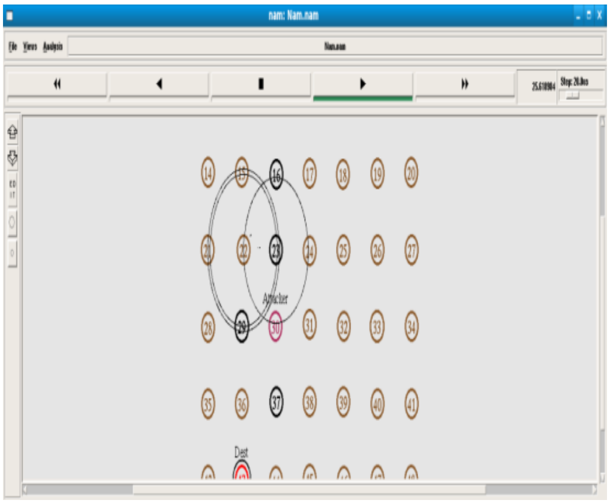

Fig.2. Attacker Generation

b) **Alternative path selection Process**
Here after finding the attacker, the packet chooses the alternative path to reach the designation from source.

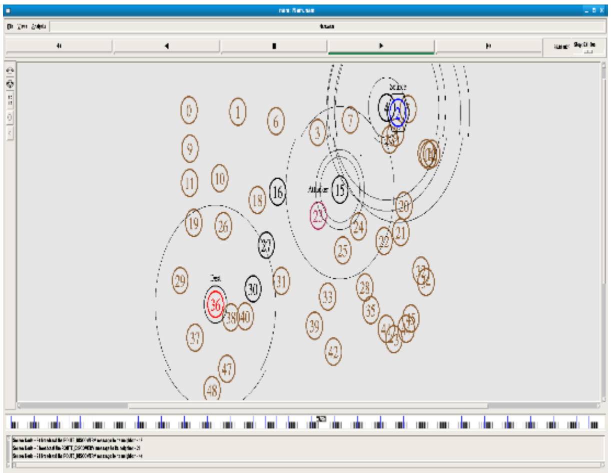

Fig.3. Alternative path selection

C) Alternate Path selections using Dynamic Non-linear authenticator Protocol

Here after finding the attacker, the packet chooses the alternative path to reach the designation from source by using the DNAP

Packet Delivery Ratio (PDR) is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source mobile node. It can be evaluated in terms of percentage (%). This parameter is also called "success rate of the protocols", and is described as follows:

$$\mathbf{PDR} = \left(\frac{\mathbf{SendPacketno}}{\mathbf{Receivepacketno}}\right) \times \mathbf{100}$$

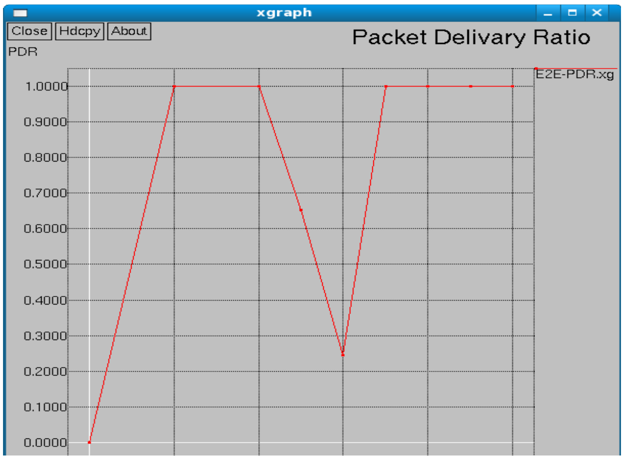

Fig.4. Packet Delivery Ratio

Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. Formula: (X=C/T) to calculate the throughput.

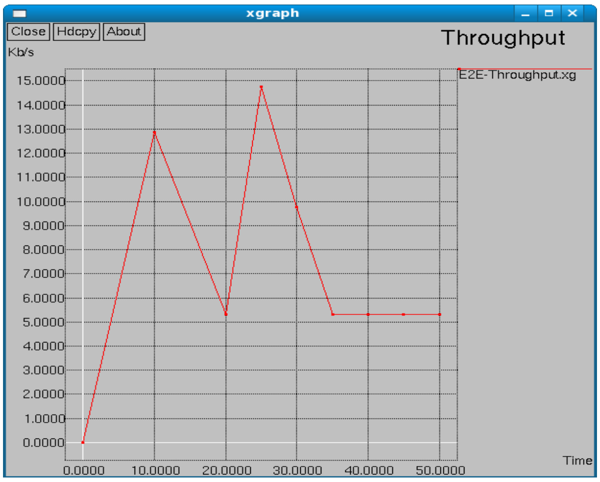

Fig.5. Throughput

Comparison Ratio Average end-to-end delay comparisons of existing methods signify how long it will take a packet to travel from source to destination node. It includes delays due to route discovery, queuing, propagation delay and transfer time.

$$D_{end-end} = N(d_{trans} + d_{prop} + d_{proc})$$

Where $D_{end\text{-}end}$= end-to-end delay, d_{trans}= transmission delay, d_{prop}= propagation delay, d_{proc} = processing delay, d_{queue}= Queuing delay and N= number of links.

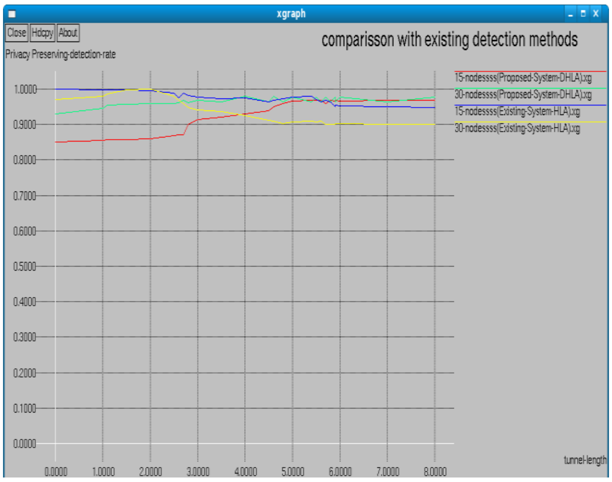

Fig.6. Comparison

V. CONCLUSION

The goal of this research is to show that compared with conventional detection algorithms that utilize only the distribution of the number of lost packets, exploiting the correlation between lost packets significantly improves the accuracy in detecting malicious packet drops. Such improvement is especially visible when the number of maliciously dropped packets is comparable with those caused by path errors. To correctly calculate the correlation between lost packets, it is critical to acquire truthful packet-loss information at individual nodes.

DOI 10.17148/IJARCCE.2016.51015

(DNAP) based routing privacy preserving protocol auditing architecture that ensures truthful packet-loss reporting by individual nodes. This architecture is collusion proof, requires relatively high computational capacity at the source node, but incurs low communication and storage overheads over the route.

REFERENCES

[1] J. N. Arauz, “802.11 Markov channel modeling,” Ph.D. dissertate ion, School Inform. Sci., Univ. Pittsburgh, Pittsburgh, PA, USA, 2004.

[2] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proc. ACM Conf. Comput. andCommun. Secur., Oct. 2007, pp. 598–610.

[3] G. Ateniese, S. Kamara, and J. Katz, “Proofs of storage from homomorphic identification protocols,” in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319–333.

[4] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, “ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks,” ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

[5] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, “ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks,” ACM Trans. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.

[6] K. Balakrishnan, J. Deng, and P. K. Varshney, “TWOACK: Preventing selfishness in mobile ad hoc networks,” in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.

DOI 10.17148/IJARCCE.2016.51015