ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Distributed Homomorphic Linear Authenticator Privacy Preserving Algorithm in MANET

A. Gowsi Monica[1], A. Indhumathi[2]

M. Phil Scholar, Department of Computer Science, Dr. SNS Rajalakshmi College of Art and Science College, Coimbatore, Tamil Nadu, India

Assistant Professor, Department of M.C.A, Dr. SNS Rajalakshmi College of Art and Science College, Coimbatore, Tamil Nadu, India

ABSTRACT: Security is one of the most important issues that have attracted a lot of research and development effort in past few years. In multi-hop wireless ad hoc network link error and malicious packet dropping are two sources for packet losses. The packet losses are caused by link errors and malicious drop are to be identified by observing a sequence of packet losses in the network. In this paper, proposed a Distributed homomorphic linear authenticator (DHLA) Privacy preserving algorithmimprove the detection accuracy to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, develop a Routing path selection (RPD) based Distributed homomorphic linear authenticator (DHLA) Privacy preserving algorithm architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This architecture is privacy preserving, collusion proof, and incurs low communication and storage overheads. Through extensive simulations and verification proposed mechanism achieves significantly better detection accuracy than conventional methods such as a privacy preserving strategy based detection.

KEYWORDS: MANET; Routing model; RPD; Authentication

I. INTRODUCTION

In a multi-hop wireless network, nodes cooperate in relaying/routing traffic. An adversary can exploit this cooperative nature to launch attacks. For example, the adversary may first pretend to be a cooperative node in the route discovery process. Once being included in a route, the adversary starts dropping packets. In the most severe form, the malicious node simply stops forwarding every packet received from upstream nodes, completely disrupting the path between the source and the destination. Eventually, such a severe denial-of-service (DoS) attack can paralyse the network by partitioning its topology. Even though persistent packet dropping can effectively degrade the performance of the network, from the attacker's standpoint such an "always-on" attack has its disadvantages. First, the continuous presence of extremely high packet loss rate at the malicious nodes makes this type of attack easy to be detected. Second, once being detected, these attacks are easy to mitigate. For example, in case the attack is detected but the malicious nodes are not identified, one can use the randomized multi-path routing algorithms to circumvent the black holes generated by the attack, probabilistically eliminating the attacker's threat. If the malicious nodes are also identified, their threats can be completely eliminated by simply deleting these nodes from the network's routing table.

Hybrid wireless networks are networks in which any mobile node in a wireless network may have connectivity, either directly or via a gateway node, to an infrastructure network. This latter network may be an IP network as the Internet, a 3G wide area wireless network, or an 802.11 local area wireless network. Actually, any other network technology may be considered. In this context, the notion of Intra technology and Inter technology appears. If a mobile node communicates with another network of similar technology, this can be seen as Intra technology hybrid wireless network. As for example, the case of a mobile node in an ad hoc 802.11 network communicating with an 802.11 Access Point (AP) in an infrastructure network. On the other hand, if a mobile node communicates with another network of different technology, this can be seen as Inter technology hybrid wireless network. As for example, the case

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

of a mobile node in an 802.11 network communicating with a 3G network. Moreover, hybrid wireless networks may integrate both Intra and Inter technology cases and the mobile node itself may support heterogeneous technologies switching between them in an on-demand fashion.

The rest of this paper is organized as follows. In Section 2 review the existing related work. The proposed models and descriptions are described in Section 3. Finally conclude the paper in Section 4.

II. RELATED WORK

In [4] authors addressed the problem of selective jamming attacks in wireless networks. In these attacks, the adversary selectively targets specific packets of "high" importance by exploiting his knowledge on the implementation details of network protocols at various layers of the protocol stack. To illustrated the impact of selective jamming on the network performance by illustrating various selective attacks against the TCP protocol.In [5] authors addressed the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. To illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. In [6] authors studied the data delivery mechanisms that can with high probability circumvent black holes formed by these attacks. To argued that classic multipath routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once the adversary acquires the routing algorithm, it can compute the same routes known to the source, hence, making all information sent over these routes vulnerable to its attacks.In [7] authors utilized and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, to further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. In [8] authors addressed the problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi-hop ad hoc networks. To develop a comprehensive system called Audit-based Misbehavior Detection (AMD) that effectively and efficiently isolates both continuous and selective packet droppers. In [9] authors proposed a novel method of energy-conserving route protocol called NCE-DSR(Number of times nodes send Constraint Energy DSR). Based on DSR protocol, mark related to the number of times of sending message is added to the datagram for routing protocol. And the nodes with relatively more number of times of sending message are protected. Cost function for route is designed for route choice with reasonable energy allocation for the whole network.

III. PROPOSED ALGORITHM

In a multi-hop wireless ad hoc network, packet losses are attributed to harsh channel conditions and intentional packet discard by malicious nodes. In this paper, while observing a sequence of packet losses are interested in determining whether losses are due to link errors only, or due to the combined effect of link errors and malicious drop. To especially interested in insider's attacks, whereby a malicious node that is part of the route exploits its knowledge of the communication context to selectively drop a small number of packets that are critical to network performance.

A. *NETWORK MODEL*

The NS2.34 simulations are evaluated in networks of 49 nodes. As the number of nodes in the ad hoc network is increased, the size of the simulation area is also increased so that a consistent node density is maintained. The simulation areas are 330m x 330m, 670m x670m and 1000m x1000m, respectively. All mobile nodes move according to the random waypoint mobility model. Node speeds are randomly distributed between zero and the maximum speed 20 m/s. The pause time is consistently 10 seconds. The maximum transmission range of each mobile node is 200 meters. If the distance between two mobile nodes is larger than 200m, they cannot communicate with each other directly. Each data point represents an average of 10 runs with the same traffic models, but different randomly generated mobility scenarios. The second set of simulations examines the performance of the two routing schemes with different percentages of Internet (wired) traffic. All traffic is CBR traffic with 512 byte data packets at the sending rate of 10 packets per second. All the sources are within the ad hoc network; the correspondent nodes are either within the ad hoc network or reachable through the wired network..

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

B. ***ROUTING MODEL PROCESS***

The routing model process mechanism is initiate whenever a node wishes to send or contact a destination node which isn't in its transmission range therefore it must obtain a route to that node by launching the Route discovery mechanism. Normally the sender must first search this route in its route cache if there is no route it proceeds as follow:

- It creates a route request packets containing its address and the address of the destination node then it broadcast this packet to all its neighbours using flooding.
- Each neighbour when receiving this request consults its cache to find an eventual route to this destination to be returned back to the sender otherwise it rebroadcast the same route request to all its neighbours after adding its address to the header of the route request and learns from this request information to be added to its cache. If the node has already treated this route request it ignores the new received request by verifying its sequence number since each route request is identified by a unique sequence number.
- The same procedure is executed by each neighbouring node until the route request arrives to destination which adds its address at the end of the header and sends a route reply.

C. ***ROUTING PATH DETECTION PROTOCOL***

Routing path detection protocol selection based on the shortest path is usually energy saving optimized. So different metrics are considered and weight is assigned to each link. Between two end-to-end nodes, there usually exists more than one route. In the potential relay node set, there will be relatively energy-optimal routes that can achieve the least cost based on the nodes' battery capacity and propagation loss of the links. The research work have a simple multi-hop Hetro-network, with the relay node set R between the source and destination, and the immediate neighbour set *R** for each node. There exists an energy efficient route, for example, the route with relay nodes *A*, *B*, and *C*. Links with less propagation power loss and nodes with higher residual battery capacity are preferred. So the problem is simplified to minimize the power consumed during transmission and maximize the battery capacity of the next node to be used that is to minimize:

$$\frac{p(i)}{(g(i)} \quad i \in \Re^* \qquad eq.(1)$$

for local (the immediate next hop) optimization

$$\sum_{i\in\Re} \frac{p(i)}{g(i)} \qquad i \in \Re \qquad eq.(2)$$

for global (all end-to-end hops) optimization where *g(i)* is the residual battery capacity of the *i*th node, and *p(i)* is the power cost per packet from node *i*-1 to node *I* (that it, Joules per second per packet). A detailed study of the Lithium-Ion battery discharging property is presented. The voltage decrease and the battery capacity are non-linear functions of discharging time: the lower the capacity remains, the faster the battery voltage drops. The residual battery capacity can be evaluated as the amount of energy remains in the battery, that is, the time duration for the battery to discharge when the transmitter is consuming power.

D. ***DISTRIBUTED HOMOMORPHIC LINEAR AUTHENTICATOR (DHLA) PRIVACY PRESERVING ALGORITHM***

DHLA routing selects 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 behaviour and state dependency in order to avoid congestion and to achieve optimal performance.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

IV. PSEUDO CODE

Algorithm: Distributed homomorphic linear authenticator (DHLA) Privacy preserving Algorithm

Input: SourceNode***S,***Destination Node ***D***, Packet Size ***P*** , Nodes ***N,*** Attacker ***A***

Output: Privacy preserving alternate path searching packet delivery

Initialize

Step 1:*IfS<D* it will

Send REQ message to all its neighbour nodes

else

choose appropriate *S* and *D*

Step 2: *ifN* == REQ message

Broadcast packet's ID to *N*

else

Cache the packet will be discarded.

Step 3: Tocalculate its energy by using:

Enew = Etx - Er + Eth + Em + Eover

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: Initialize ***A*** in the routing path

Step 7: Choosing alternate path will send privacy preserving message to its own neighbours and this process will be continued till the destination node reaches.

V. SIMULATION RESULTS

The proposed simulation accepts the simulation parameters as input which contains the NS2.34 simulation where the novel Trust based secure graph detection algorithm is applied to the mobile AdHoc network.Packet delivery Ratio (PDR): the ratio of the data packets delivered to the destinations to those generated by the Constant Bit Rate (CBR) sources. The EPDR shows how successful a protocol performs delivering packets from source to destination. The higher for the value give use the better results. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness.

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:

$$PDR = \left(\frac{SendPacketno}{Receivepacketno}\right) \times 100 \qquad eq.(3)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

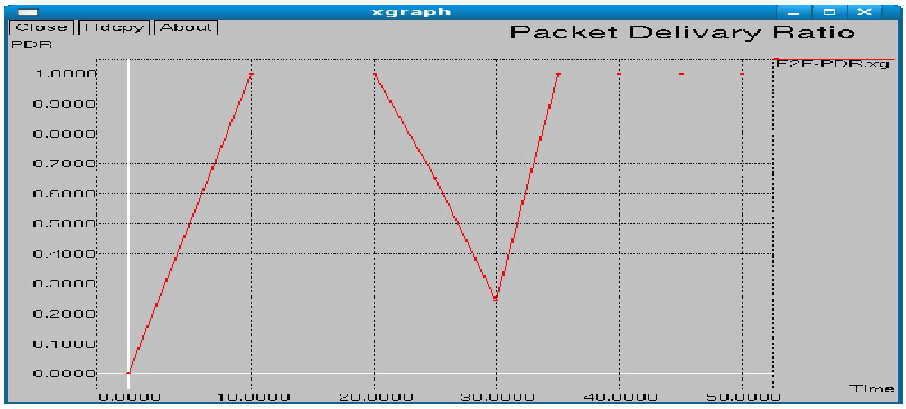

Fig.1. Packet delivery Ratio (PDR)

Data Packet Drop (Packet Loss): Mobility-related packet loss may occur at both the network layer and the MAC layer. Here packet loss concentrates for network layer. When a packet arrives at the network layer. The routing protocol forwards the packet if a valid route to the destination is known. Otherwise, the packet is buffered until a route is available. A packet is dropped in two cases: the buffer is full when the packet needs to be buffered and the time that the packet has been buffered exceeds the limit. That is, in most cases it is impossible to design an optimal packet dropping scheme based on transmission durations alone, as the full energy function is required. This is very different from the single deadline case, in which the optimal transmission durations do not depend on the packet size or energy function. It is often of interest to limit the maximum transmit power, which is determined by the minimum transmission duration of the minimum subgroup. Moreover, in scenarios when the minimum subgroup is outweighed in energy contribution by another group (or subgroup), the difference in contribution by these two groups typically is not significant. An asymptotically optimal dropping scheme is a packet dropping scheme which results in the minimum average transmission energy as the packet size approaches infinity.

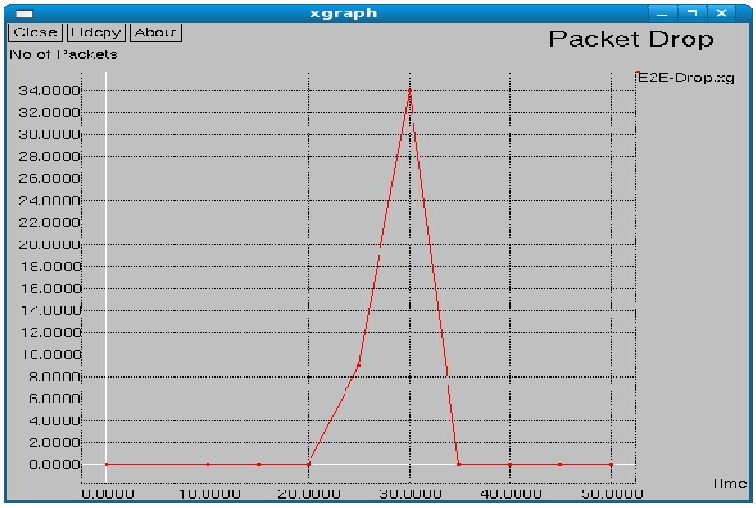

Fig. 2. Data Packet Drop (Packet Loss)

VI. CONCLUSION AND FUTURE WORK

The NS 2.34 simulation results showed that the proposed algorithm is designed, implemented and evaluated a multi-hop ad hoc network using privacy preserving secure Distributed homomorphic linear authenticator (DHLA) algorithm in NS 2.34 Framework. Each secure alternate routing path communicates wirelessly with another using the IEEE

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

802.11b technology without any aid of infrastructure. The main protocol implemented in this application was the DHLA algorithm, which consists of two important mechanisms, alternate routing path selection and prevention of packet dropping. The future work A malicious packet dropping detection technique that effectively detects the packet dropping attack in any environment while keeping the generated overheads minimal will be focus.

REFERENCES

1. J. N. Arauz, "802.11 Markov channel modeling," Ph.D. dissertation, 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. and Commun. 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. A. Proano and L. Lazos, "Selective jamming attacks in wireless networks," in Proc. IEEE ICC Conf., 2010, pp. 1–6.
5. A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," IEEE Trans. Depend. Secure Comput., vol. 9, no. 1, pp. 101–114, Jan./Feb. 2012.
6. T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.
7. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM Conf., Mar. 2010, pp. 1–9.
8. Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," IEEE Trans. Mobile Comput., PrePrint, Vol. 99, published online on 6 Sept. 2013.
9. Linyang Sheng, Jingbo Shao, Jinfeng Ding "A Novel Energy-Efficient Approach to DSR Based Routing Protocol for Ad Hoc Network" 2010 IEEE.