IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 1, January 2017

Study on Homomorphic Linear Authenticator in Wireless Ad Hoc Networks

Kapil M. Patel[1], Sushant S. Bahekar[2]

PG Student, Department of Computer Engineering, SSBT's COET, Bambhori, Jalgaon, India [1]

Assistant Professor, Department of Computer Engineering, SSBT's COET, Bambhori, Jalgaon, India [2]

Abstract: In wireless ad hoc network, there are two sources for packet loss i.e. link errors and malicious packet dropping. It is important to determine whether the losses are caused by link errors only, or by combined effect of link errors and malicious drop. Here, we are especially interested in the insider attacker case where malicious nodes drops packet selectively to degrade the network performance. Packet dropping rate in the insider attack case is nearly equal to normal link error because of which existing algorithms cannot find the exact reason of packet loss. We are going to find the correlation between lost packets and to ensure that these correlations are accurate we are going to use Homomorphic Linear Authenticator (HLA) based public auditing mechanism. The HLA architecture is privacy preserving and collusion proof.

Keywords: Packet loss, Truthful detection, Homomorphic Linear Authenticator, Cryptography.

I. INTRODUCTION

In wireless ad hoc network, nodes communicate with each other via wireless links either directly or relying on other nodes as routers. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network. An adversary may misbehave by agreeing to forward packets and then failing to do so. Once being included in a route, the adversary starts dropping packets. That means it stop forwarding the packet to the next node. The malicious node can exploit its knowledge about the protocol to perform an insider attack. It can analyze the importance of the transmitting packet and can selectively drop those packets. Thus it can completely control the performance of the network.

If the attacker continuously dropping packets, it can be detect and mitigate easily. Because even if the malicious node is unknown, one can use the randomized multi-path routing algorithms to circumvent the black holes generated by the attack. If the malicious nodes get identified, the node can be deleted from the routing table of network. The detection of selective packet dropping is highly difficult. Sometimes the dropping of packets may not be intentional. It can be occurred as a result of channel errors. So the detection mechanism should be capable of differentiating the malicious packet dropping and the dropping due to link errors.

The algorithm introduced here provides an efficient mechanism to detect the selective packet dropping. It improves the detection accuracy by calculating the correlation between lost packets with the help of Auto Correlation Function of the bitmaps at each node in the route. Bitmap describes the lost/received status of each packet in the transmission. The basic idea is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the correlation pattern is different.

To get the correct correlation, the truthfulness of the packet loss bitmaps is essential. In order to ensure the correctness the system uses a public auditing mechanism. The auditor uses a variation of the cryptographic primitive called homomorphic linear authenticator (HLA) [1].It is a signature scheme widely used in cloud computing and storage server systems, which allows client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it [2]. Indirect reciprocity is a powerful mechanism for the evolution of cooperation between nodes. The essential concept of indirect reciprocity is "I help you not because you have helped me but because you have helped others" [3].

II. RELATED WORK

Based on how much weight a detection algorithm gives to link errors relative to malicious packet drops, the related work can be broadly divided into the following to categories.

- High malicious dropping rates
- Number of maliciously dropped packets is more link errors

A. High Malicious Dropping Rates

This category is having those systems that has high malicious dropping rate where almost all packets are dropped because of malicious packet dropping. Here the

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 1, January 2017

link errors are neglected. This category is further divided into four sub-categories where each sub-category works depending upon some system. The four systems for four sub-categories are described as follows:

1) Credit System
In this type of system, a node receives credit by sending packets for other nodes. These credits are used by nodes to send its own packets [4]. If a malicious node is continuously dropping the packets then it will lose credits and it cannot send its own traffic.

2) Reputation Systems
The second sub-category is based on reputation systems [5], [6], [7], [8]. Here the system depends on neighbour nodes to identify the malicious node. A node which drops most of the packets will get a bad reputation by its neighbour node. This information is passed to all the nodes in the network and is used to select routes for the next packet transmission. A high packet dropping node is eliminated fromthe routes.

3) End-to-End or Hop-to-Hop Acknowledgements
The third sub-category relies on end-to-end or hop-to-hop acknowledgements to directly locate the hops where packets are lost.

4) Cryptographic Methods
This sub-category is used to construct the proofs for the forwarding of received packet at each node.

B. Number of Maliciously Dropped Packets is More Than Link Errors
The second categoryis having high malicious packet dropping rate than the link errors, but here effect of link error is not neglected. Here source traffic rate and estimated received rate are calculated and are compared with each other. If the difference between these two is within a range then packet dropping is because of link errors and if the range is high then packet dropping is because of malicious node.

C. Disadvantages

- Themost of the related works assumes that malicious dropping is only source of packet dropping.
- For the credit-system-based method, a malicious node may still receive enough credits by forwarding most of the packets it receives from upstream nodes.
- In the reputation-based approach, the malicious node can maintain a reasonably good reputation by forwarding most of the packets to the next hop.
- While the Bloom-filter scheme is able to provide a packet forwarding proof, the correctness of the proof is probabilistic and it may contain errors.
- As for the acknowledgement-based method and all the mechanism in the second category, merely counting the number of lost packets does not give a sufficient ground to detect the real culprit that is causing a packet loss.

III.PROPOSED SYSTEM

Consider a multi-hop network which is having an arbitrary path P_{SD}as shown in fig. 1. The source node sends thepackets through intermediate nodes to the destination node. In each hop, the sending node is called as an upstream node of an receiving node. The packets are transmitted from source to destination and a bitmap is obtained for each node as $(a_1,a_2….a_m)$ where a_j=0 or 1. If the packet is successfully transmitted then a_j=1 and if the packet is not transmitted the value of a_j is considered as 0. By using this bitmap we can find the correlation between the lost packets. From this correlation we can find the malicious node.

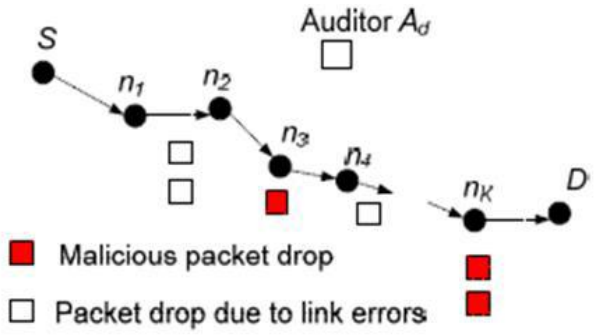

Fig. 1. Network and Attack Model

There is an auditor in the network which is independent. The meaning of independent is that it is not related with any of the nodes in the network and it doesn't know about the secrets associated with the nodes. Here auditor is capable of detecting attacker's node when it gets request from the source. After sending all the packets from source to destination, the destinationsends a feedback to source about the route i.e. whether the route is under attack or not by considering some parameters. After getting feedback, if the route seems to be under attack then source will send the attack detection request (ADR) to auditor. Now auditor starts investigation to find malicious node. The auditor requests certain information from the intermediate nodes . Here normal nodes reply with correct information and the malicious node try to cheat. Here each and every node must reply for the auditor request otherwise the node is considered to be misbehaving.

The main challenge here is for the guaranty of the information sent by the nodes to the auditor. The attacker usually sends the wrong information not to get detected. Sometimes the malicious node may drop the packet and will send that that the packet is transmitted. To overcome this problem we are using Homomorphic linear authenticator (HLA) a cryptographic method which is used in cloud computing. In this type of scheme, source is allowed to generate the HLA signatures $s_1,…,s_M$for M

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 1, January 2017

messages $r_1,\ldots,r_M$. The source sends these signatures s_i's and packets r_i's along the route. The node will create a valid HLA signature if and only if it has received all the signatures. Since s_i's and r_i's are sent together, the reception of signature sensure that all the packets are transmitted without getting dropped. In this way we can truthfully detect the malicious node.

A. Scheme Details

The system consists of four phases which are listed below:

- Setup Phase
- Packet Transmission Phase
- Audit Phase
- Detection phase

1) Setup Phase

This phase takes place immediately after the route is established, but before the any data packets are propagated over the route. The source node decides on symmetric-key crypto- system for encryption the packet during the transmission phase. Source securely allocates a decryption key and a symmetric key to each node on the path. Key allocation may be based on the public-key crypto-system. The source node also announces two hash functions to each node in the route. Apart from this, source also wants to set up its HLA keys.

2) Packet Transmission Phase

Once Setup phase completed successfully, source node enters into the transmission phase. In packet transmission phase, before the transmission of packets source node computes the hash value of every packet and generates HLA signatures of the hash value for each node. These signatures are then sent together with the packets to the route by using a one-way chained encryption.

This mechanism prevents the deciphering of the signatures for downstream nodes by the upstream node. When a node in the route receives the packet from source it extracts packets and signature. After that it verifies the integrity of received packet. A database is maintained at each node on route. It can be considered as a FIFO queue which records the reception status for the packets sent by source. Each node stores the received hash value and signature in the database as a proof of reception.

3) Audit Phase

Audit phase is triggered when the public auditor receives an attack detection request (ADR) message from source node. This ADR message consist of the id of the nodes on route, ordered in the downstream direction, source's HLA public key information, the sequence numbers of most recent packets sent by source, and the sequence numbers of the subset of these most recent packets that were received by destination. The auditor requests the packet bitmap information from every node in the route by issuing a challenge. From the information stored on the database, each node generates this bitmap. Auditor checks the validity of bitmaps and accepts if it is valid. Otherwise it rejects the bitmap and considers the node as a malicious one.

Note that this mechanism only guarantees that anode cannot understate its packet loss, i.e., it cannot claim the reception of a packet that it actually did not receive. This mechanism cannot prevent a node from overly stating its packet loss by claiming that it did not receive a packet that it actually received. This latter case is prevented by the mechanism based on reputation which is discussed in the detection phase.

4) Detection Phase

The public auditor enters in the detection phase after receiving and auditing the reply to its challenge from all the nodes on route. Auditor constructs per hop bitmaps and by using an auto correlation function (ACF) it will find out the correlation between the lost packets. After thatit finds out the difference between the calculated value and correlation value of wireless channel. Based on the relative difference, it decides whether the packet loss is due to the malicious node or link error. When it finds out malicious drop, it can consider both ends of the hop as suspicious. That means either the transmitter did not send the packet or receiver did not receive.

After identifying these two suspicious nodes, the detector needs to find out the actual culprit. For this, it can check the reputation value. Now the Auditor module will collect the reputation value for the two suspicious nodes. When a node fails to forward the packet it, it will get minimum reputation. By checking this, the detector can easily distinguish the attacker.

B. Advantages of Proposed System

- High detection accuracy.
- Privacy preserving: the public auditor should not be able to decern the content of a packet delivered on the route through the auditing information submitted by individual hops.

C. Disadvantages of Proposed System

- Data confidentiality will raise the issue in this work.
- Due to signature generation overhead may be high.

IV. CONCLUSION AND FUTURE SCOPE

In this paper correlations of lost packets are correctly calculated. To ensure the truthfulness of information send by the nodes. HLA based public auditing architecture is used to provide privacy preserving and collision avoidance. For future work we can use different methods to generate keys for thegeneration of signatures to reduce overhead and we can use some encryption method to obtain data confidentiality. We can add one signature to the block of packets to the instead of adding one signature to reduce the overheads.

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 1, January 2017

REFERENCES

[1] C. Ateniese, 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.

[2] 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.

[3] M. A. Nowak, and K. Sigmund, "Evolution of indirect reciprocity," Nature, vol. 437, pp. 1291-1298, Oct. 2005.

[4] T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim. "Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks",In Proceedings of the IEEE ICC Conference, 2009, pp. 1062–1067.

[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. Inform. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

[6] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," In Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw.Comput. Conf., 2002, pp. 226–236.

[7] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable secure routing for ad hoc networks," In Proc. IEEE INFOCOM, Mar. 2010, pp. 1 –9.

[8] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation-based incentive scheme for ad hoc networks," In Proc. IEEE Wireless Commun. Netw. Conf., 2004, pp. 825–830.

[9] Tao Shu and Marwan Krunz, "Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks," IEEE Transactions on Mobile Computing, Vol. 14, No.4, April 2015.

[10] A. Proano and L. Lazos. "Packet-hiding methods for preventing selective jamming attacks", IEEE Transactions on Dependable and Secure Computing, 9(1):101–114, 2012.

[11] Aejaz Ahmed, H c Sateesh Kumar, "HLA Based Public Auditing Architecture to Find Malicious Node in Ad Hoc Network-A Review,"International Journal of Research in Science & Engineering, Vol. 1. pp. 325-328.

[12] Sneha C.S and Bonia Jose, "Detecting Packet Dropping Attack In Wireless Ad Hoc Networks," International Journal on Cybernetics & Informatics (IJCI) Vol. 5, No. 2, April 2016, pp. 118-124.

[13] Monika Nag K J and Mr. S. Lokesh, "Detecting Truthfullness of Packet Dropping Attacks Using Public System In Wireless Ad Hoc Network," International Journal for Scientific Resaerch & Development (IJSRD)Vol. 3, April 2015, pp. 176-178.