DETECTION OF LINK ERROR AND ATTACK IN ADHOC NETWORK

Jagadesh.G[1], Sherlin.S[2], Mrs.Jeyaselvi.M[3]

Student, Dept. of Computer Science and Engineering, Agni College of Technology, India.[1,2]

Asst. Professor, Dept. of Computer Science and Engineering, Agni College of Technology, India. [3]

ABSTRACT:-

An Ad hoc Wireless Networks are defined as the category of wireless networks that utilize multihop radio relaying and are capable of operating without the support of any fixed infrastructure. Link Error and Malicious packet dropping are the major two issues in Wireless Ad hoc Networks. To reduce the amount of Link Error and Malicious packet dropping an auditor node is setup to monitor the entire Wireless Ad Hoc Network. This reduces a sequence of packet loss in the network. Malicious node route exploit their knowledge to the neighbouring nodes to selectively drop a small amount of packets critical to the network performance. The packet loss can be identified by Homomorphic Linear Authenticator (HLA) based public auditing scheme. This setup is implemented in AODV routing protocol with RREQ and RREP. This algorithm improves the performance of entire Wireless Network by detecting the malicious node and to avoid them and provides reliable transmission in Wireless packet delivery

***Keywords*-HLA, ADR message, Auditor,AODV, RREQ,RREP**

1. INTRODUCTION

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. Wireless Ad-hoc networks are rapidly gaining popularity as a mode of communication, especially among highly mobile sectors of society.

To reduce the malicious attack and whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop. We are especially interested in the insider-attack case, whereby malicious nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance.

Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network. In this paper, while observing a sequence of packet losses in the network, we are interested in determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop.

We are especially interested in the insider-attack case, whereby malicious nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy.

To improve the detection accuracy, we propose to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, we develop a homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes.

This construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead of the baseline scheme, a packet-block-based mechanism is also proposed, which allows one to trade detection accuracy for lower computation complexity. Through extensive simulations, we verify that the proposed mechanisms achieve significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection.

2. SYSTEM ANALYSIS

EXISTING SYSTEM

In existing system we analyse link error and malicious attacks in network. The credit-system-based method, a malicious node may still receive enough credits by forwarding most of the packets it receives from upstream nodes.Similarly, in the reputation-based approach, the malicious node can main- tain a reasonably good reputation by forwarding most of the packets to the next hop. The Ellip- tic Curve Digital Signature Algorithm (ECDSA) cryptographic method is used in this existing method.

LIMITATIONS:

- lost packets are caused by malicious dropping.
- In an open wireless environment, link errors are quite significant

Proposed System

The proposed mechanism is based on detecting the correlations between the lost packets over each hop of the path. The basic idea is to model the packet loss process of a hop as a random process alternating between 0 (loss) and 1 (no loss). we develop a homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes.

3. IMPLEMENTATION

HLA based public auditing architecture

The proposed mechanism is based on detecting the correlations between the lost packets over each hop of the path. Here detection architecture consists of four phases.

1. Setup.
2. Packet transmission.
3. Audit.
4. Detection.

i)Setup Phase :

In this phase, Source decides on a symmetric-key crypto-system and K symmetric keys. Key distribution may be based on the public-key crypto-system such as RSA. Besides symmetric key distribution, S also needs to set up its HLA keys.

ii)Packet Transmission Phase :

After completing the setup phase, Source enters the packet transmission phase. The special structure of the one-way chained encryption construction in dictates that an upstream node on the route cannot get a copy of the HLA signature intended for a downstream node .

iii)Audit Phase :

This phase is triggered when the public auditor receives an ADR message from Source. This mechanism only guarantees that a node cannot understate its packet loss 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.

iv)Detection Phase :

The public auditor enters the detection phase after receiving and auditing the reply to its challenge from all nodes. The main tasks of auditor in this phase include the following: detecting any overstatement of packet loss at each node, con- structing a packet-loss bitmap for each hop, calculating the autocorrelation function for the packet loss on each hop, and deciding whether malicious behavior is present.

3.2 ADHOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV routing is an algorithm use for finding a route for peer to peer connection between sensors. AODV relies on a broadcast route discovery mechanism, which is used to dynamically establish route table entries at intermediate nodes. Each senors as router and routes are obtain only when needed. AODV will broadcast route request (RREQ) to all and whoever in the range of the frequency being transmitted and awake, they can receive RREQ. Any sensor which meets the information in the RREQ will answer RREQ with route reply (RREP). After the sender gets the RREP, it now has the peer-to-peer connection and ready to send.

The path discovery process of AODV is initiated whenever the source node needs to transmit data to another node, but for which the source node does not have routing information in its table. Each node in the network maintains its own sequence number. A source issuing an RREQ packet also includes its own sequence number and most recent sequence number it has for the destination. Therefore intermediate nodes reply to an RREQ only if the sequence number of their route to the destination is greater or equal to the destination sequence number specified in RREQ packet.

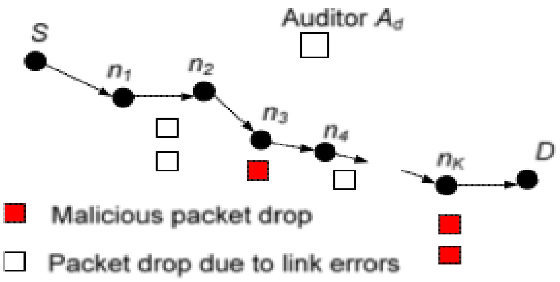
AODV primary objectives are:

1. To broadcast discovery packets only when necessary.
2. To distinguish between t local connectivity management and general topology maintenance.

Advantage of AODV:

AODV is the simplest and widely used algorithm either for wired or wireless network. The advantages of bandwidth efficiency loop free routing and act as a reactive protocol makes it worth to apply within the network. They provide access to information and services regardless of geographic position. Independence from central network administration. Self-configuring network, nodes are also act as routers. Less expensive as compared to wired network.

4. SYSTEM ARCHITECTURE



5. PERFORMANCEEVALUATION

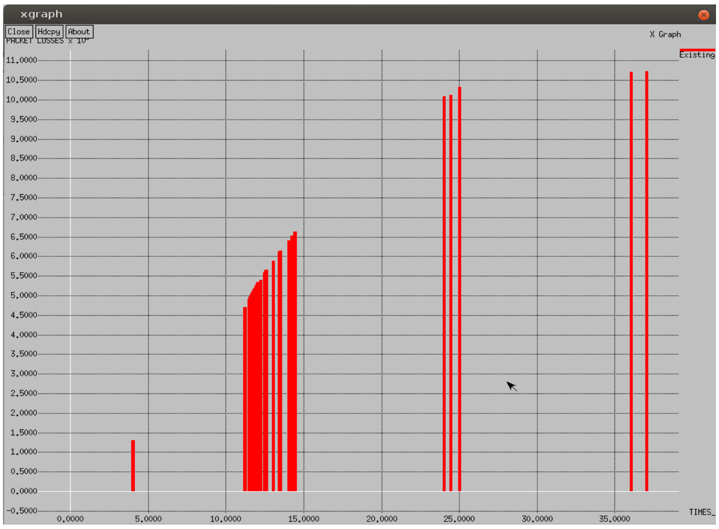
In this section, we evaluate the performance of simulation. We are using the xgraph for evaluate the performance.

We choose the three evaluation metrics:

- **Packet loss** - **Th**e number of packet loss at destination and number of packet sent by the source.
- **Delay** -The average time taken for a packet to be transmitted from the source to destination.
- **Throughput**-Number of data received by the destination without any losses.

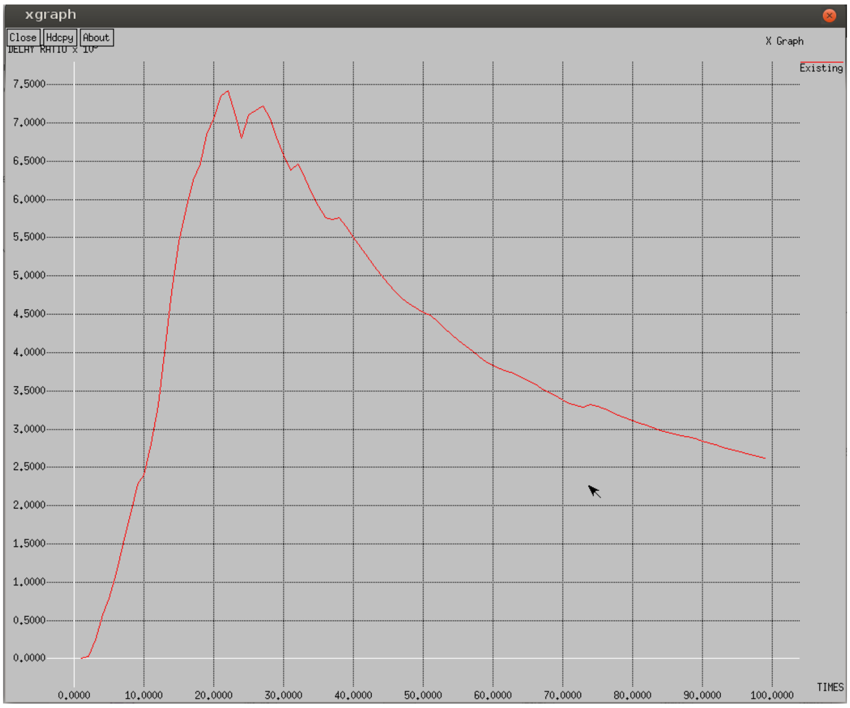
Packet loss ratio:

Only 20% of packet drop has occurred by dynamically fixing an Auditor node in Wireless Network.



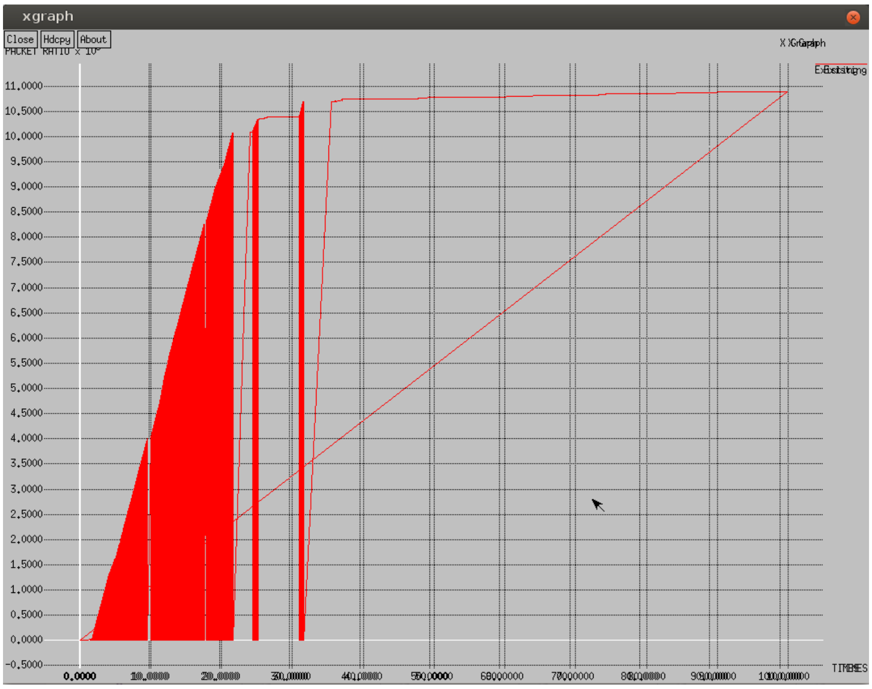
Delay ratio:

35% of delay has occurred in packet transmission.



Throughput:

80% of packet has reached the destination without any packet loss.



6. CONCLUSION

In this paper we have assumed that source and destination are truthful in following the established protocol because delivering packets end-to-end is in their interest. 80% of packet has reached their destinations without any loss by implementing HLA algorithm and cryptosystems.Moreover, in this paper, as a proof of concept, we mainly focused on showing the feasibility of the proposed cypto-primitives and how second order statistics of packet loss can be utilized to improve detection accuracy. Some open issues remain to be explored in our future work.

REFERENCE:

1. 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.
2. 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.
3. 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,.
4. Y. Zhang, L. Lazos, and W. Kozma, “AMD: Audit-based misbe-havior detection in wireless ad hoc networks,” IEEE Trans. Mobile Comput., PrePrint, Vol. 99, published online on 6 Sept. 2013.
5. A. Proano and L. Lazos, “Selective jamming attacks in wireless networks,” in Proc. IEEE ICC Conf., 2010, pp. 1–6.