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

Detection of Packet Losses in a Network by using Collision Method

Regalagadda Sambasiva[1], Renuka Kondabala[2]

M Tech, Dept. of I.T., CNIS, VNR VJIET, Bachupally, Hyderabad, Telangana, India[1]

Assistant Professor, Dept. of I.T., VNR VJIET, Bachupally, Hyderabad, Telangana, India[2]

ABSTRACT: Packet losses in a network play a significant role in determining packet dropping in multi-hop wireless ad hoc networks. The two factors responsible are malicious packet dropping and link error. The packet losses can be due to one of the above factors or a combination of both. In this paper we are determining the factor that is responsible for packet losses. This could be due to nodes that are part of the path which is responsible for dropping of packets to affect the performance of the network. To do this we are finding out the relations between lost packets. For this a Homomorphism Linear Authenticator (HLA) is proposed for truthful calculations of relation between connecting nodes. The HLA verifies the truthfulness of the information about packet loss from the nodes, which follows the architecture of public auditing. It provides collision proof, privacy preserving and allows low overheads. In this paper we fix the inner attack by the intruder and find the node that is responsible for the attack.

KEYWORDS: Node, Routing, Homomorhism, Authenticator, Sampling, Stealth, Collision.

I. INTRODUCTION

The nodes in multi-hop wireless networks collaborate in routing traffic [1]. This can be used as a weakness by the intruder or attacker to launch attack. The intruder can misguide user by pretending himself as a cooperative node in finding or discovering route. Once the intruder accesses the route and gets himself included in the route, he starts to drop the packet. This node slowly stops to block the path of each and every other node. This, in severe or extreme instance conditions the node completely stops the forwarding of each and every packet from source and the destination. This is one type of denial of service attack which separates the network from its topology.

This kind of continuous attack on the network has advantages and disadvantages. The advantage being is continuous attack at only one node makes itself easily detected. Following the attack can be easily neutralized. If, for example, the attack is found to be happened and the place where the attack is not identified then the user can choose different routing algorithms so that the black holes identified can be avoided to remove threats. The threats generated by these nodes can be avoided by excise these nodes fully.

The attacker node is a member of the route can launch an attack as an insider with perception of network protocol and the context of communication. This can cause the same damage as the persistent attacker [2] as a stealth. This node drops the valuable packet that his more importance in the functioning of the network. By targeting important packets the damage can be very high with catching probability to be less. This paper deals with such kind of intruder and restricting the attack. We are identifying the problem why the selecting packets are dropping and the nodes that are responsible for the dropping of packets. This is very hard in dynamic wireless networks. This is very hard due to the fact that we need not only find the hop where the packet is dropped but also need to find whether the dropping is done intentionally or unintentionally. As the wireless networks now-a-days are open natured, the dropped packets may be due to bizarre conditions such as noise, fading, interference etc or due to insider. The insider can disguise himself in weak conditions of the network. The packet loss rate cannot be a entity for identification for exact cause.

In the current work we are developing an algorithm that is accurate in the detection of selective drop of packets that is caused due to the insider attack. Our work also provides truthful and decision statistics that are verified publicly. The accuracy is high due to the fact that we are utilizing the correlations. The Auto- correlation Function (ACF) is calculated by taking the locations of lost packets. Hence this method is used to detect the exact reason for packet loss. This can be due to the combination of affects of malicious drop and link error. The proposed algorithm takes into account of cross statistics of lost packets so as take a more informative decision.

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

One of the main challenges in our work will be the truthfulness of packet-loss reports of bitmaps which indeed gives the status of transmission of each and every packet. This is highly important for correct calculation. Hence an auditing method is required for verifying truthfulness of information. The solution we are proposing for auditing here is Homomorphic Linear Authenticator (HLA). HLA is a signature schema in cloud. The storage server systems used this mechanism as a proof from severs to trusted clients. HLA which we are proposing is a collision proof that is different from conventional HLA which has experienced a number of problems when the malicious node collides and exchange information. This result in making the auditor gets confused due to upstream and downstream malicious nodes. Hence, due to this the packet dropping gets undetected.

We are also including the properties like privacy preserving by not allowing the auditor to change the content of information given by individual hops. The communication overheads are lowered along with storage. This helps our system to be usable to be for a number of wireless devices including sensors. We are proposing an algorithm for packet blocking that helps in the generation of signatures and its detection. This helps in improving accuracy where the complexity is low.

II. RELATED WORK

The work is divided into two modules. The first module deals with dropping rates of packets due to malicious dropping. The link errors are eliminated here as most of the work is related to this module. This first module is subdivided into four categories for identifying attacking nodes. The credit system comes into first category where it provides impulse for cooperation. The credit is received by node by relaying packets. This is used by node to send its own packets. Hence the intruder decreases the dropping of packets and consumes his own credit [3]. This results in the elimination of sending his own traffic. The second sub category is the reputation system on which the user relies on. This system helps in the monitoring of neighbours which give users about the information of misbehaving nodes. The node that drops packets at high is given bad reputation. It is used as a path in selecting routes. Thereby, this malicious node can be removed from the route. The third sub module is related to one to one or end to end connection. This helps in finding the route where the connection is lost. Similarly it is also eliminated. The fourth sub module is solving the problem by using cryptography.

The second category deals with the dropped packets that are malicious are high in number where the link error influence is low. The knowledge of wireless networks is necessary in this case. The traffic rate is estimated by sampling packet arrival. We compare the traffic of source with the received traffic.

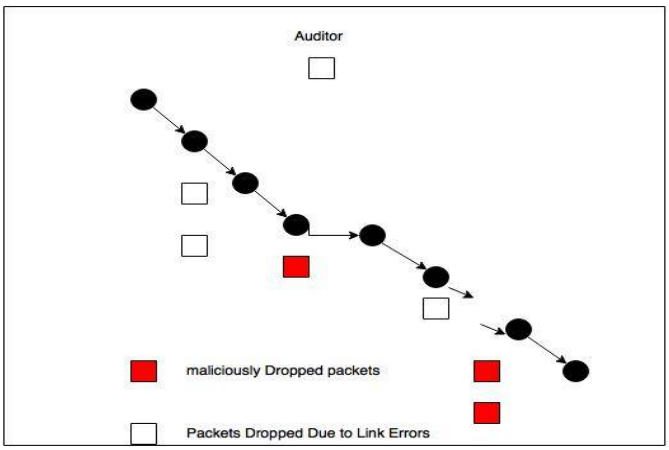

Fig 2.1 Architectural Diagram of Proposed Approach

The methods proposed did not work in high traffic that is selected. The reputation system can also be faltered by maintaining good reputation. The accuracy of the previous work algorithms may decrease in case of highly selected malicious drops.

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

Our project dealt with above faults. The problems in the previous papers are being addressed in this paper.

III. EXISTING SYSTEM

The existing system works on modules. It can be divided into two modules. It deals with high dropping malicious rates and ratio of maliciously dropped packets to link errors. The first module is further divided into four sub modules. They are credit systems, cryptographic methods, end-to-end acknowledgements, reputation systems. The disadvantages Include assuming that only source is malicious dropping for packet loss, the nodes in upstream and downstream are equal, the intruder node can have a good reputation, very hard to come to conclusion that who is the real culprit in acknowledgement based method.

IV. PROBLEM STATEMENT

The identification of nodes that act maliciously is identified. The auditor should verify the behaviour of malicious [5] node to be questionable with proof. This should be privacy preserving so that the data satisfies Integrity. The proposed system has low communication overheads and storage overheads which can be used by various wireless networks.

V. PROPOSED SYSTEM

We propose a system which works on the mechanism of detection of correlation between each hop where the packets are lost. The hop is alternated between 0 and 1. By transmitting a sequence of packets between 0 and 1. 0 denotes for loss and 1 denotes for No Loss. The system ensures that packet loss mentioned by the nodes is correct. It gives the status of each packet. The auditing mechanism is proposed which examines the truthfulness of given information. The system ensures that the public auditor will not be able to see the information present in the packet. For this we give HLA and Auto Correlation Function [6]. Advantages of proposed system are privacy preserving, overheads are low in communication and storage servers, collision proof HLA construction, computation overhead, a prediction algorithm for packet blocking for detection and signature generation.

VI. IMPLEMENTATION

The implementation of current algorithm is done in four phases. The four phases are initialization phase, packet transmission phase, Auditing phase and Detection Phase.

Initialization phase:

This path should be established to start this phase. After this the data is transmitted through this route. The source node is responsible for encrypting the packet before sending it to destination. At destination the packet is verified and hence decryption is followed.

Packet transmission phase

After initialization phase, Packet Transmission phase is started. The packet is transmitted from source to destination. The HLA signatures are generated for nodes. The authentication used here is MAC and code is generated using Hash function. If the verification fails in transmission the node should stop sending packet.

Auditing Phase

It is started when the auditor starts the reception of message from source. It includes the ID in downstream direction. The HLA signature is generated in the auditing process.

Detection Phase

In the detection phase the packet with malicious node is detected in the auditing. In this phase the packet checks for consistency of bitmaps. The normal node gives the truthful information of packets which is not unique with the packets at reported by malicious node. the packets which are lost are denoted by 0 and which are not lost are denoted by 1. This kind of detection process applies to one end-to-end scheme. The public verifiability is done after each detection. We require no knowledge of HLA [8] key that is used for generation of keys. This should ensure that the data is confidential in overall communication process.

The communication overhead and storage overhead is minimal in this work. It is a onetime cost incurred in this process.

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

VII. SIMULATION RESULTS

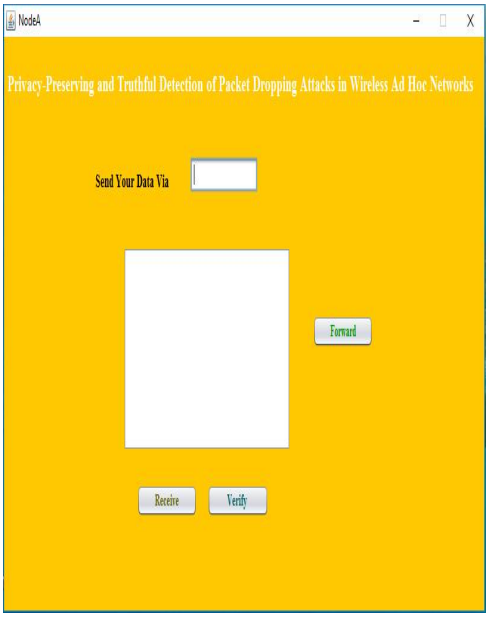

Fig 7.1 Node A

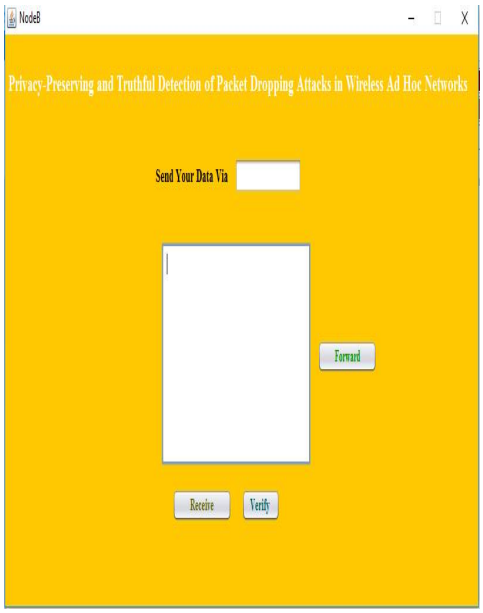

Fig 7.2 Node B

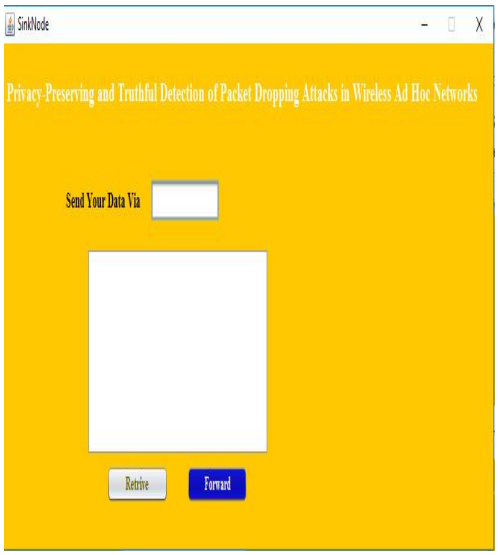

Fig 7.3 Sink Node

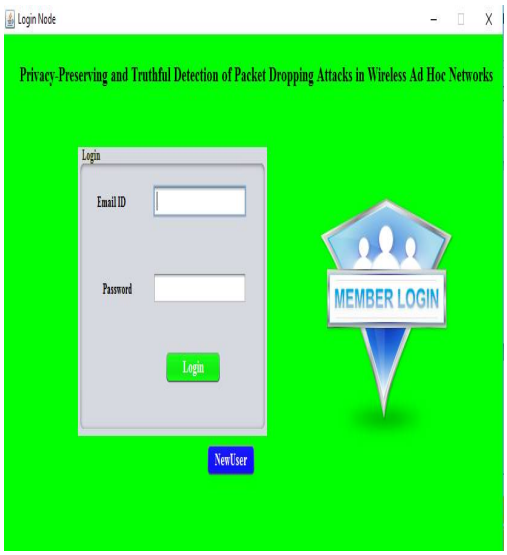

Fig 7.4 Login Node

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

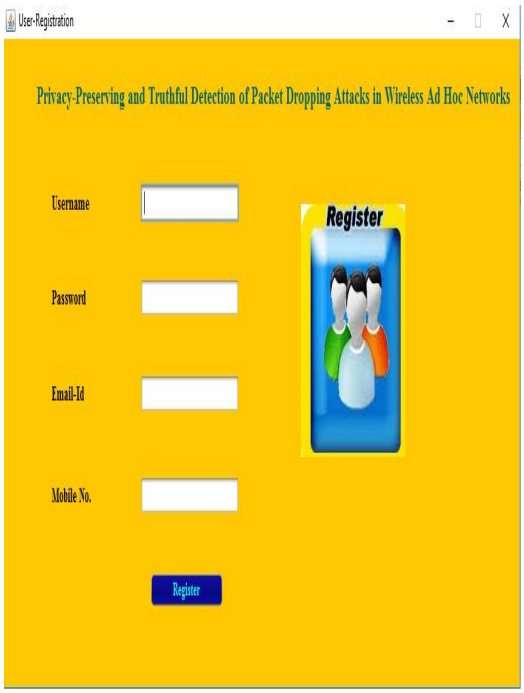

Fig 7.5 User Registration

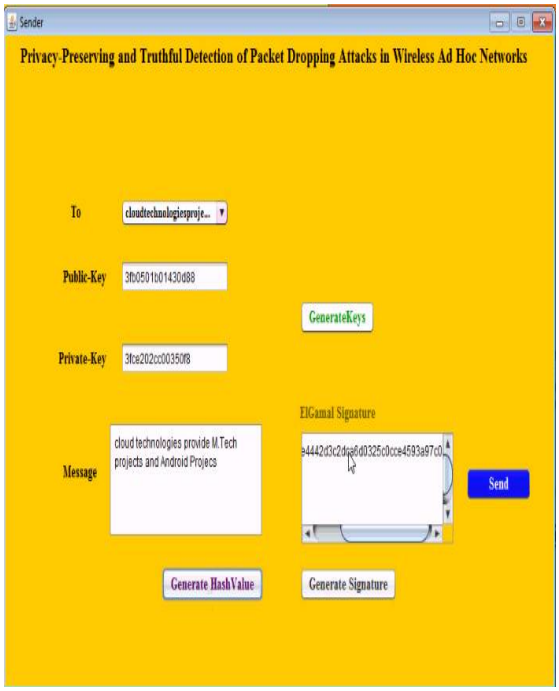

Fig 7.6 Along with public Key and Private Key

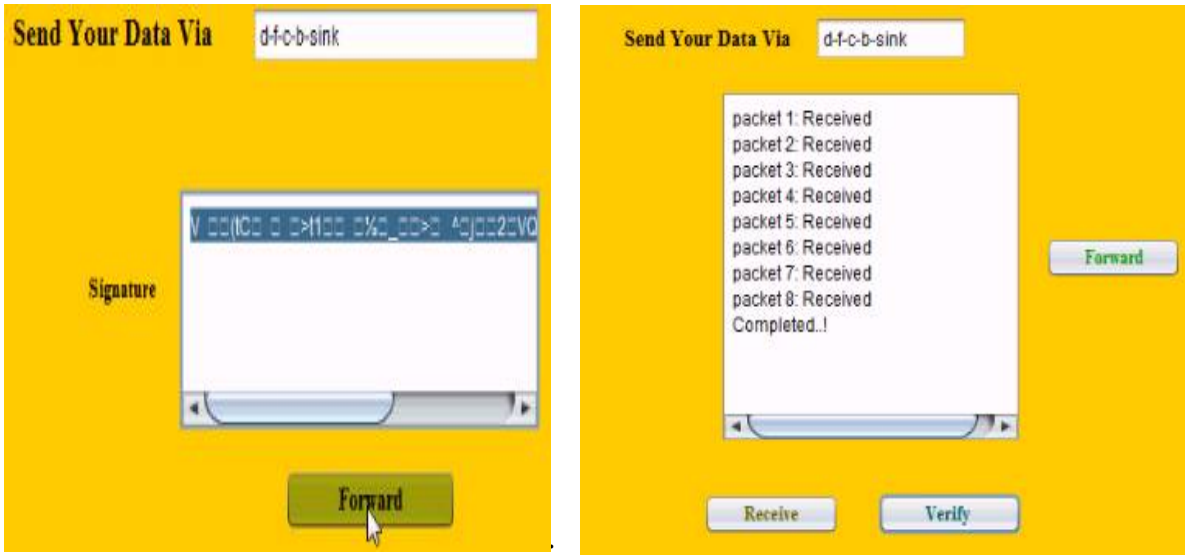

Fig 7.7 Data Sending and receiving packets in network

VIII. CONCLUSION

When compared to existing algorithms which use only no of lost packets distribution the use of correlation improves the accuracy in the detection of loss of packets. It is quite evident from the Ratio of lost packets due to malicious packets to correlation packets. To do this, truthful information is needed which is done by the HLA. It is collision proof system. A packet block based mechanism is proposed to ensure to reduce overhead computation which increases overall accuracy.

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

IX. FUTURE WORK

The proposed system is a static one which can be implemented dynamically. The network topology can be changed frequently which is not considered. The proposed systems are used only low wireless environments. It can be implemented for high mobile environment. The proposed method can be optimized for various protocols.

REFERENCES

[1] G.Ateniese, S.Kamara and J. Katz proofof storage from Homomorphic Identificationprotocols. In proceedings of the internationalconference on the theory and application ofcryptology and information security.
[2] G. Noubir and G. Lin. Low power DoSattacks in WLANS and countermeasures.
[3] B. Awerbuch, R. Curtmola, D. Holmer,C. Nita-Rotaru, and H. Rubens. ODSBR: anon-demand secure byzantine resilient routingprotocol for wireless ad hoc networks. ACMTISSEC, 10(4), 2008.
[4] D. Boneh, B. Lynn, and H. Shacham.Short signatures from the Weil pairing.Journal of Cryptology, 17(4):297–319, Sept.2004.
[5] S. Buchegger and J. Y. L. Boudec.Performance analysis of the confidantprotocol (cooperation of nodes: fairness indynamic ad-hoc networks). In Proceedings ofthe ACM MobiHoc Conference, 2002.
[6] L. Buttyan and J. P. Hubaux.Stimulatingcooperation in self-organizing mobile ad hocnetworks. ACM/Kluwer Mobile Networks andApplications, 8(5):579–592, Oct. 2003.
[7] J. Eriksson, M. Faloutsos, and S.Krishnamurthy.Routing amid colludingattackers. 2007. International Journal of Computer Techniques - Volume 2 Issue 2, Mar
[8] W. Galuba, P. Papadimitratos, M.Poturalski, K. Aberer, Z. Despotovic, and W.Kellerer. Castor: Scalable secure routing forad hoc networks. In INFOCOM, 2010Proceedings IEEE, pages 1 –9, march 2010.