Secure Routing Using Hla on Wanet To Detect The Packet Loss

Vundamati Udayabala[1], P. Naga Deepthi [2]& Marlapalli Krishna[3]

[1]Student of M.Tech.(CST), Dept. of CSE, Sir C R Reddy College of Engineering, Eluru, India

[2]Assistant Professor, Dept. of CSE, Sir C R Reddy College of Engineering, Eluru, India

[3]Senior Assistant Professor, Dept. of CSE, Sir C R Reddy College of Engineering, Eluru, India

Abstract: - Packet droppings are usual attacks occurring in Wireless Ad hoc Network (WANET). This menace occurs when the data is transmitted from one source to destination. The assailment may be relegated into two types - one is malevolent packet dropping and another one is due to link errors. This can be overcome by implementing Homomorphic Linear Authenticator (HLA). It is the public auditing scheme to detect the maleficent node in WANET. HLA acts like an auditor to detect the packet losing schemes in the network. The main advantage of this scheme is to securely transmit the data in WANET. The packet dropping rate is commensurable to the channel error rate, conventional algorithms that are predicated on detecting the packet loss rate cannot reach acceptable detection precision. To amend the detection precision, correlations between lost packets are identified. HLA predicated public auditing architecture is developed to verify the veracity of the packet loss information reported by nodes. Thus the implementation is utilizable to eschew packet dropping attacks in Wireless Ad hoc Network.

Key words: Packet dropping, secure routing, Homomorphic linear signature, auditing

1. INTRODUCTION

In Wireless Ad hoc Network, nodes are co operatively function in routing path. An assailant utilizes this cooperation and pretends to be a one of the nodes in the routing path. Once the assailant included in the routing path commences discarding the packets. The intrusion node ceases sending the packet received from the above node to the node below which consummately perturb the routing path between the sender and receiver. This type of assailment is kenned as Denial of Service (DoS). The maleficent node may relegate the paramountcy of different packets and discard the most paramountcy packets which lead to degradation of the network performance the authors in [3], [4], [5] Identifying the consequential packet is a critical task in a wireless medium. In this paper, I develop an absolute algorithm for identifying the most consequential packet discard made by the inside intruder. The algorithm provides veracious and publicly verifiable decision by the auditor. The precise detection is obtained by the correlations between the lost packets. The correlations are performed by Auto correlation function [ACF]. To verify the lost packets and the information sent by the individual node about the packet loss is checked by constructing Homomorphism Linear Authenticator [HLA]. HLA is a signature scheme that provides privacy, collusion avoidance and low storage overheads. Anterior work on distinguishing between causes for dropped packets considered only collisions and channel errors [2], [5] and ignored malevolent packet drops. On the other hand, protocols that detect malignant packet dropping [6], [8] ignored collisions and channel errors. In this paper, I adopt an amalgamated approach to packet loss considering collisions, channel errors, and maleficent packet drops.

2. RELATED WORK

The work is relegated into two categories. First category is predicated on malignant node dropping the packet which works on detecting the malevolent node that causes the discarding of packets. Detection precision of malevolent node is done by four ways i) whenever a node sends a packet it will earn a point for transmitting a packet. The malignant node which perpetually discards the packet will lose its point [2] [1] [6] ii) Each node is monitored by its neighbor node. So the misconducting node is monitored by the neighbor node iii) malignant node place will be identified and abstracted from the network iv) Some cryptographic method is utilized to have the record of forwarded packets. All these ways of identifying the maleficent node have disadvantages and these methods will not be applicable when the packets are highly selective.

The main conception is that shorter RTS/CTS and MAC headers in 802.11 are less vulnerably susceptible to errors than data. Thus, during the RTS/CTS access procedure, errors are postulated to be due to collisions. If the node receives the CTS frame but not the ACK frame, then the transmission has more likely failed due to a channel error. However, if an RTS/CTS frame is not received, then the transmission more likely failed due to a collision. If a fundamental access procedure is utilized, the sender depends on feedback from the receiver to determine the cause of packet loss. If a packet with a corrupted header is received, the receiver sends nothing and the sender will timeout and surmises that a collision occurred. If a packet with a correct header is received but the data part is corrupted, the receiver can apperceive the sender and reply with a NAK frame. Here, the sender will surmise that the packet was disoriented due to channel error.

2.1 EXISTING SYSTEM:

The most of the cognate works preclude the ambiguity of the environment by postulating that malignant dropping is the only source of packet loss, so that there is no desideratum to account for the impact of link errors. On the other hand, for the minute number of works that differentiate between link errors and maleficent packet drops, their detection algorithms conventionally require the number of malevolently-dropped packets to be significantly higher than link errors, in order to achieve acceptable detection precision. Depending on how much weight a detection algorithm gives to link errors relative to malignant packet drops, the cognate work can be relegated into the following two categories. The first category aims at high malevolent dropping rates, where most (or all) lost packets are caused by malevolent dropping. The second category targets the scenario where the number of malevolently dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible.

DISADVANTAGES OF EXISTING SYSTEM:

In an open wireless environment, link errors are quite consequential, and may not be significantly more minuscule than the packet dropping rate of the insider assailer. So, the insider assailer can camouflage under the background of astringent channel conditions. In this case, just by observing the packet loss rate is not enough to accurately identify the exact cause of a packet loss. This quandary has not been well addressed in the subsisting system. In the subsisting system first category case, the impact of link errors is ignored. In the second category case, certain erudition of the wireless channel is indispensable.

2.2 PROPOSED SYSTEM:

In this paper, I develop a precise algorithm for detecting selective packet drops made by insider assailants. The algorithm withal provides a veracious and publicly verifiable decision statistics as a proof to fortify the detection decision. The high detection precision is achieved by exploiting the correlations between the positions of lost packets, as calculated from the Auto-Correlation Function (ACF) of the packet-loss bitmap—a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions. The fundamental conception abaft this method is that even though malevolent dropping may result in a packet loss rate that is commensurable to mundane channel losses, the stochastic processes that characterize the two phenomena exhibit different correlation structures (equipollently, different patterns of packet losses). Ergo, by detecting the correlations between lost packets, one can decide whether the packet loss is pristinely due to customary link errors, or is a cumulated effect of link error and maleficent drop. The algorithm takes into account the cross-statistics between lost packets to make a more informative decision, and thus is in sharp contrast to the conventional methods that rely only on the distribution of the number of lost packets.

ADVANTAGES OF PROPOSED SYSTEM:

The proposed system with incipient HLA construction is collusion-proof. The proposed system gives the advantage of privacy-preserving. The construction incurs low communication and storage overheads at intermediate nodes. This makes the mechanism applicable to a wide range of wireless contrivances, including low-cost wireless sensors that have very inhibited bandwidth and recollection capacities. This is additionally in sharp contrast to the typical storage-server scenario, where bandwidth/storage is not considered an issue. Lastly, to significantly reduce the computation overhead of the baseline constructions so that they can be utilized in computation-constrained mobile contrivances, a packet-block-predicated algorithm is proposed to achieves scalable signature generation and detection. This mechanism sanctions one to trade detection precision for lower computation involution.

3. IMPLEMENTATION

A. Network Model:

The wireless channel as shown in Figure 1, in which the source node perpetually sends packets to the destination node through intermediate nodes n1……nk (where n is the upstream node of ni+1), is modeled of each hop along P (Path to Source and Destination) as a desultory process that alternates between good and deplorable states. Packets transmitted during the good state are prosperous, and packets transmitted during the deplorable state are disoriented. A sequence of M packets is transmitted over the channel**.**

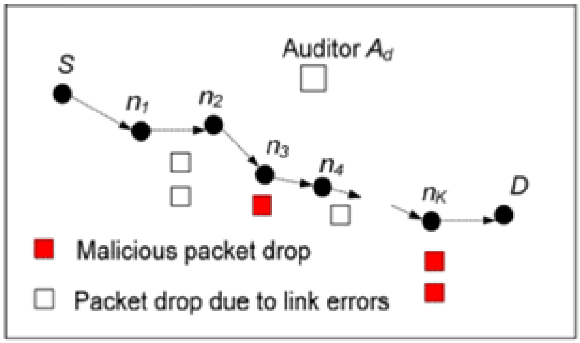

Fig:-1 Network Model

B. Independent Auditor:

There is an independent auditor Ad in the network. Ad is independent in the sense that it is not associated with any node in P. The auditor is responsible for detecting maleficent nodes on demand. Categorically, it is postulated S receives feedback from D when D suspects that the route is under attack. After receiving feedback, S sends ADR to Ad, A commences to identify the packet loss. To facilitate its investigation, Ad needs to accumulate certain information from the nodes on the route.

C. Setup Phase:

This phase takes place right after path P is established, but afore any data packets are transmitted over the route. In this phase, Source node encrypts the packet and sends to destination through intermediate nodes. After receiving the packets destination node can verify the packets and after verification it can decrypt the packets.

4. CONCLUSION

In this paper, correlations of lost packet are correctly calculated. To ascertain the veracity of information send by the nodes HLA predicated auditing architecture is utilized to provide privacy preserving, collision avoidance and low communication storage overheads. Extension to dynamic environments will be studied in future work.

5. 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.