International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June-2017 www.irjet.net p-ISSN: 2395-0072

PRIVACY PRESERVING AND DETECTION TECHNIQUES FOR MALICIOUS PACKET DROPPING IN WIRELESS ADHOC NETWORKS

Anjaly Joy[1]

[1] *Anjaly Joy,M TECH Student, Computer Science and Engineering, Rajadhani Institute of Engineering and Technology, Kerala, India*
[2] *L M Bernaldu, HOD, Computer Science and Engineering, Rajadhani Institute of Engineering and Technology, Kerala, India*

Abstract - *Wireless Ad Hoc Network are network with no infrastructure where nodes collaborate in supporting the network functionality. The effect of malicious nodes lead to Packet Dropping and will disrupt the communications of between nodes within the ad hoc network. Link errors cause packet dropping, so does the insider attack, or the combined effect of link errors and malicious nodes cause packet dropping. 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. Conventional algorithms based on detecting the packet loss rate cannot achieve satisfactory detection accuracy because the packet dropping rate is comparable to the channel error rate. Hence to improve the detection accuracy, the correlations between lost packets is identified. This paper presents a study on packet dropping attacks and their detection based on auto correlation function.*

Key Words: *Packet Dropping, Link Errors, Wireless adhoc networks, auto correlation function.*

1. INTRODUCTION

The wireless ad hoc network is a collection of mobile nodes with no fixed infrastructure, nodes searches for a route from source to a destination. Thus the dynamic and distributed environment is exploited, which requires the collaboration among nodes. Due to the inherently vulnerable nature of wireless ad hoc network trust between the nodes is an issue, in order to communicate or collaborate with each other. While all the information is delivered through many hops, eavesdropping, forging or dropping during transmission can occur.

Thus the cooperative nature of wireless Ad hoc network can be exploited to launch attacks. A network level denial-of -service (Dos) attack, physical layer jamming attacks brings a security breach in the wireless network. Denial of service attacks aims at the complete disruption of routing and therefore the whole operation of wireless network. Whereas, in case of an Information Disclosure attack, the compromised node may leak confidential information to unauthorized nodes which includes information regarding network topology, location of nodes or optimal routes to unauthorized nodes. In a black hole attack, a malicious node advertises itself as having a valid route to the destination. The attacker consumes or intercepts the packet without forwarding. This cause the network traffic diverted or dropped. Persistent packet dropping attacks can degrade the performance of the network.

The solution based on identifying or isolating the misbehaving nodes that refuses to forward packets in a wireless ad hoc networks are classified on the basis of selective and random packet dropping. Once the detection of malicious node is attained, randomized multi-path routing algorithms can reduce the effect of insider attacks. Their threats can be completely eliminated by simply deleting the nodes from the network's routing table. The challenge faced in the detection of selective packet dropping attacks is the highly dynamic nature of wireless environment.

The requirement of focusing the location (or hop) the packet is dropped and to identify whether the drop is intentional or not. The main reason for packet drop in the network is due to bad channel conditions such as fading, noise, interference or the link errors or by the insider attack. Link errors are significant in packet dropping considering the insider attack which can camouflage the technique of packet loss rate.

The packet loss rate cannot accurately identify the cause of a packet loss. The correlations between the positions of lost packets is exploited to achieve high detection accuracy. It can be calculated from the auto-correlation function (ACF) of packet-loss bitmap (bitmap describes the lost/received status of each packet in a sequence of consecutive packet transmissions). Based on the correlation between the lost packets, one can decide the reason for packet drop

The packet-loss bitmaps reported by individual nodes along the route may not be truthful, so it become more challenging to guarantee the truthfulness. Such truthfulness is essential for correct calculation of the correlation between lost packets. This challenge is not important, because it is a common practice of an attacker to report false information in order to avoid detection accuracy.

2. LITERATURE REVIEW

Literature review provides us with various techniques for detecting malicious packet drops. Also, various classification techniques have been adopted by the authors.

R. Rao and G. Kesidis proposed a paper titled "Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks" which observes packet dropping attacks by detecting the traffic pattern.

The traffic intensity is checked by using sensors. A traffic transmission patterns is used to find traffic rate for receiver to verify the traffic .This traffic patterns are used with MAC to preserves the statistical regularity from node to node. This general technique for intrusion detection is only suitable for networks that are not bandwidth limited and thus the proposed system cannot be implemented in a bandwidth limited networks.

L. Buttyan and J. P. Hubaux, proposed a paper titled "Stimulating cooperation in self organizing mobile ad hoc networks" where a credit system which provides an incentive for cooperation.

Here each node receives credit by relaying packets for one node to another, and uses its credit to send its own packets. As a result the malicious node that drop packets and will eventually deplete its credit, so that it cannot be able to send its own traffic. For explaining about the cooperation among mobile nodes Dynamic Source Routing (DSR) protocol is used. The security Module prevents counter from being negative or being modified which is the main advantage discussed over here and it is very expensive to integrate it.

Tao Shu, Sisi Liu and Marwan Krunz proposed a paper titled, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes" discussed about a multipath scheme.

Here an adversary acquires the routing algorithm and using this information the adversary node compute the same routes known to the source, and hence make interruption to all information sent over these routes. The adversary cannot identify the routes traversed by each packet. The routes generated by these mechanisms are highly dispersive and energy-efficient. A mechanism for randomized multipath routes is explained in this paper, but it is highly expensive to conduct its simulations..

S.Marti, T.Giuli, K.Lai and M.Baker proposed a paper titled, "Mitigating Routing Misbehavior in Mobile Ad hoc Network", discussed about a reputation system that relies on neighbors to monitor and identify misbehaving nodes.

Node with high packet dropping rate is given a bad reputation by its neighbors and this Reputation information is propagated periodically throughout the network and is used as an important metric in selecting routes. And finally a malicious node will be excluded from any of the route. Dynamic Source Routing (DSR) protocol which uses source routing without relying on routing table. The ambiguous collision among the misbehaving node is ailed to be detected in this paper.

Alejandro Proano and Loukas Lazos proposed a paper titled, "Packet-Hiding Methods for Preventing Selective Jamming Attacks" where the problem of jamming under an internal threat model is discussed.

The adversary will be aware about the network secrets and the implementation details of network protocols. For launching selective jamming attacks in network the adversary node will exploit the internal knowledge of network. In this case the adversary will remain active only for a short period of time which aims on messages of high importance. The packet hiding methods are based on several cryptographic primitives. Hence the computational and communication overhead become the main issue.

K. Liu, J. Deng, P. Varshney, and K. Balakrishnan proposed a paper titled, "An acknowledgement-based approach for the detection of routing misbehavior in MANETs", discussed about an acknowledgment based system.

An end-to-end or hop-to-hop acknowledgement which directly locate the hops where packets are lost. A hop of high packet loss rate will be excluded from the route and will improve the performance rate. The receiver will send back an acknowledgment to the sender side on receiving data packets. If acknowledgment time take more time than that of wait of time then whole link will be considered to be misbehaving which turned to be challenging.

3. PROPOSED DETECTION MECHANISM

Different network metrics change simultaneously and consequently their combined effect on a specific impact. Some network metrics like packet loss and network delay change concurrently when the networking equipment's interconnect the applications. The packets are queued in buffers on traversing through the network and due to the reason of buffer overflow the packets are being dropped from time to time. The cause of packet loss can be easily identified if the drop is made intentional and the correlation related to the lost packets from each hop of the path can also be easily be identified. Hence the proposed mechanism is based on detecting the correlation of the lost packets over each hop. The correlation of lost packets is calculated using the auto-correlation function of bitmap. The accuracy of detecting malicious node can be achieved by exploiting the correlations between the positions of lost packets. This can done by calculating the auto-correlation function (ACF) of the packet-loss bitmap (bitmap describes the lost/received status of each packet in a sequence of consecutive packet transmissions). The cause of packet drop can be detected by calculating the

correlations between lost packets. The truthfulness of packet-loss bitmaps reported by individual nodes is a major challenge faced by this system. Hence auditing is required to overcome this. Cryptographic primitive is used to reduce the burden of auditing and detection homomorphic linear authenticator (HLA). This development is privacy protect, scam proof and provides low communication overheads. Hence the proposed system provides high detection accuracy and privacy-preserving feature which is attained by a public auditor. Low communication and storage overheads at intermediate nodes are being avoided to an extent.

3. DIFFERENT PHASES OF PROPOSED SYSTEM

The proposed mechanism consists of different phases:

3.1 Key Generation Phase

Once the routes are established from source to destination, say route PSD where S forms the source and D forms the destination. Source decides a symmetric-key crypto system and k symmetric keys. Besides the symmetric key distribution, Source also needs to identify the HLA keys to generating the HLA signatures. The homomorphic encryption scheme was originally called a privacy homomorphism which is based on RSA. The essence of fully homomorphic encryption allows anyone to encrypt the intermediate plaintext values. No information should leak. The inputs, outputs and intermediate values are always encrypted. Key distribution is also based on the public-key crypto-system such as the RSA. Every node on PSD maintains a database which contains the proof-of-reception status. As a result, every node in the route PSD obtains the HLA signatures for all packet. These signatures are then sent together with the packet to the route by using a one-way chained encryption.

3.2 Audit Phase

The node generates a packet-reception bit-map based on the information in the database. Node submits these data to the auditor, as a proof of packets it has received. If the details given by the node are similar as that of the details provided by the bit-map then the node can be considered as legitimate. If not, that particular node which holds inequality is considered to be the malicious node. The above mechanism can only guarantee that a node cannot understate its packet loss and cannot claim the reception of a packet.

3.3 Detection Phase

The public auditor calculates the autocorrelation function for the packet loss at each hop. The ACF of the wireless channel is then compared with the ACF of the block-reception bitmap reported by each node to detect possible malicious packet drops. The bitmaps is checked by the auditor for finding any possible packet loss. The auditor starts constructing the per-hop packet-loss bitmap based on the outcome of consistency and is done sequentially from the first hop. Only the packets lost are accounted by the auditor. For deciding whether the packet loss is caused by malicious drop the auditor calculates the autocorrelation function for each bitmaps and the relative difference is observed. The HLA construction is publicly verifiable and privacy preserving so that the auditor cannot determine the content of the packets transmitted from source to destination.

3.4 Re-routing Phase

The effect of packet dropping can be re-routed after the detection of malicious node and it can be also mitigated. One of the most effective method used is Randomized dispersive routes .A suitable path is selected in a randomized manner from the set of multiple paths rather than using pre-computed set of paths, so that large number of routes can be generated for each source and destination.

4. CONCLUSIONS

Detecting malicious packet dropping is a challenging issue in networks. The conventional detection algorithms face many challenges that is best suited by the proposed approach. The accuracy in detecting malicious packet drops is achieved exploiting the correlation between the lost packets. A public auditing architecture developed by HLA which uses cryptographic primitives to ensure truthfulness and high detection accuracy. The randomized dispersive routes by detecting the malicious nodes effectively overcome. Proposed method performs well based on the experimental result. Issues due to changes in topology and link-characteristics are to be considered in future work. In this paper we have assumed the truthfulness of source and destination and also the possibility of malicious source and destination is to be considered. The collaboration of nodes can also be exploited within the nodes to increase the efficiency of the routing path chosen.

REFERENCES

[1] R. Rao and G. Kesidis, “Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited,” in Proc. IEEE GLOBECOM Conf., 2003.

[2] L. Buttyan and J. P. Hubaux, “Stimulating cooperation in selforganizing mobile ad hoc networks,” ACM/Kluwer Mobile Netw. Appl., 2003.

[3] A. Proano and L. Lazos, “Selective jamming attacks in wireless networks,” in Proc. IEEE ICC Conf., 2010.

[4] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgement- based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput.,2006.

[5] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005.

[6] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., 2010.