IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 35-40
www.iosrjournals.org

Efficient Technique for Privacy Preserving and Detection of Malicious Packet Dropping In Wireless Adhoc Networks

Hridya V Devaraj, Asst. Prof. Jinu Mohan
Final Year M Tech Dept. of Computer Science & Engineering SreeNarayanaGurukulam College of Engineering Kerala, India

Abstract: *In a Wireless Ad Hoc Network, nodes collaborate in supporting the network functionality. The effect of malicious nodes can lead to Packet Dropping, which disrupt the communications of potentially any node within the ad hoc networking domain. 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.*

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

I. Introduction

A multi-hop wireless networks are a collection of nodes that communicate with each other wirelessly by using radio signals with a shared channel. The nodes dynamically establish a connection between the source node (which forms the connection point, a redistribution point, or a communication end point) to the destination node. Nodes can act as sources, sinks and relays for packet. In a communication network, nodes can interact with each other, collaborate or even influence each other in establishing a connection.

Since the wireless adhoc network is a collection of mobile nodes with no infrastructure fixed, nodes searches for a route to a destination. Thus the dynamic and distributed environment is exploited, which requires the collaboration among nodes. Trust between nodes is an issue, in order to communicate or cooperate with each other. So the wireless ad hoc network is inherently vulnerable. 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. Such information includes the information regarding network topology, geographic location of nodes or optimal routes to unauthorized nodes in the network. 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 under selective and random packet dropping. Once the detection of malicious node is attained, randomized multi-path routing algorithms can mitigate 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.

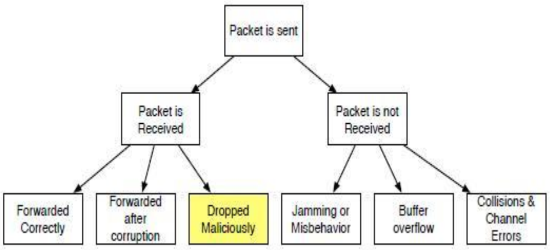

Fig 1 : Overview of packet losses

The existing solutions for identifying misbehaving nodes use per-packet evaluation of peer behavior such as the 2ACK technique which detects the misbehaving links. Per-packet behavior evaluation is based on transmission overhearing or achieving of per-packet acknowledgement. This type of monitoring operations must be repeated on every hop, thus it requires high communication overhead and energy expenditure on a multi-hop network.

The requirement of focusing the location (or hop) the packet is dropped and to identify whether the drop is intentional or not. The packet drop in the network could be caused by 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. Just observing the packet loss rate cannot accurately identify the cause of a packet loss. The high detection accuracy can be attained by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of packet-loss bitmap (describes the lost/received status of each packet in a sequence of consecutive packet transmissions). By detecting the correlation between the lost packets, one can decide whether the packet loss is purely due to link errors, or by the combined effect of malicious drop and link errors.

II. Literature Survey

In the year 2003, R. Rao and G. Kesidis proposed a paper titled “Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited” which observes the traffic patterns for the detection of packet dropping attacks. Sensors are used to check the traffic intensity. The network misinterpret the cause of packet loss as congestion instead of malicious activity. This paper suggests a traffic transmission patterns to be selected so that the verification can be made by a receiver. Such traffic patterns are used with suboptimal MAC that preserves the statistical regularity from hop to hop. This general technique for intrusion detection is therefore suitable for networks that are not bandwidth limited but have strict security requirements and thus the proposed system cannot be implemented in a bandwidth limited networks.

In the year 2010, Tao Shu, Sisi Liu, and Marwan Krunz proposed a paper titled, “Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes” where a multipath scheme is explained. So once an adversary acquires the routing algorithm, it can compute the same routes known to the source, and hence endanger all information sent over these routes. The adversary cannot identify the routes traversed by each packet. Besides randomness, the routes generated by this mechanisms are also highly dispersive and energy-efficient, making them quite capable of bypassing black holes at low energy cost. This paper, develops a mechanism that generate randomized multipath routes. But extensive simulations are to be conducted and hence this is highly expensive method.

Later on, in the year 2012, Alejandro Proan˜o and Loukas Lazos proposed a papertitled, “Packet-Hiding Methods for Preventing Selective

Jamming Attacks” In this paper, the problem of jamming under an internal threat model. The adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack is considered. The adversary exploits the internal knowledge for launching selective jamming attacks in which it targets on “high importance” messages. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. The packet hiding Methods are based on several cryptographic primitives. Hence the computational and communication overhead is an issue.

And in the year 2014 Kennedy Edemacu, Martin Euku and Richard Ssekibuule proposed “Packet drop attack detection techniques in wireless ad hoc networks: a review” which provides numerous techniques based on reputation module, route discovery module, audit module referred as the AMD system. These modules closely interact to coordinate the functions of misbehavior detection, discovery of trustworthy routes, and evaluation of the reputation of peers. The schematic on the relationship between the three modules of AMD is as shown in the figure.

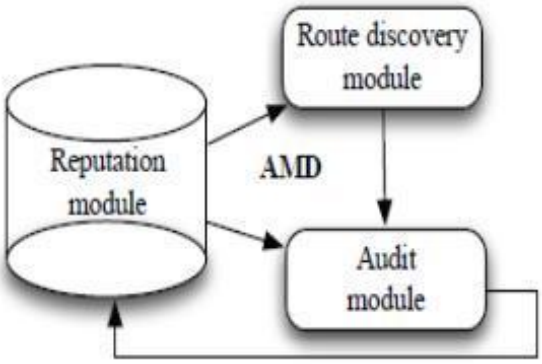

Fig 2 : AMD Architecture

The related work can be classified into the following two categories. The first category aims at the malicious packet dropping rates, which is based on the insider attacks. Here the impact of link errors is ignored. Credit systems, reputation systems, hop-to-hop acknowledgements and several cryptographic methods are used in this category.

A. The credit system provides an incentive for cooperation where the nodes receives credit by relaying packets for others. Thus the credits of malicious nodes are depleted due to the continuous drop of packets.
B. The reputation system is based on monitoring and identifying the misbehaving nodes. The neighbors are used for this purpose where the node with high packet dropping rate is given a bad reputation by its neighbors. This information is propagated throughout the network and is used as a metric in selecting routes.
C. An end-to-end or hop-to-hop acknowledgement directly locates the packet drop.
D. Cryptographic methods can also be used in identifying the malicious packet dropping rates.

The Second category is based on the number of maliciously dropped packets, but the drops caused by link errors are not negligible. Hence the source traffic rate with the estimated received rate is compared. This provides the information within a reasonable range and thus one can identify whether the drop is based on impairments or due to the malicious dropping.

Issues in conventional methods:

These methods do not perform well when the packet dropping is highly selective.

1. In the credit based method, malicious nodes can gain the credit by forwarding packets it received.
2. In a reputation-based method, similar as in previous approach the reputation can be attained by forwarding the packets to the next hop. Thus a good reputation is maintained.
3. The acknowledgement-based method and the mechanisms in the second category, focuses on counting the number of lost packets. This is not sufficient to detect the malicious node causing the packet losses.

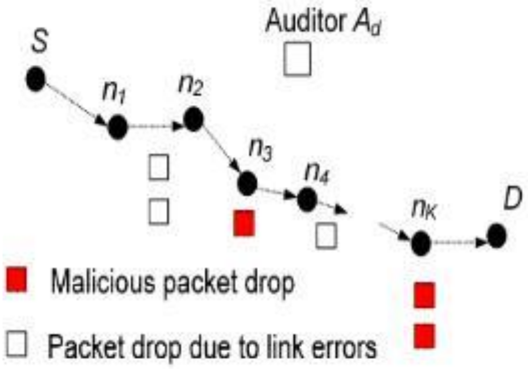

Fig 3 : Network Model

Because the packet drop is highly selective, the detection accuracy of these conventional approaches deteriorates. The packet loss can be due to link errors or the combined effect of malicious and the link error. The above figure represents the combined effect of link and malicious errors.

III. Proposed Detection Mechanism

In some scenarios the different network metrics change simultaneously and consequently their combined effect on a specific impact. Some network metrics such as the packet loss and network delay change simultaneously when the networking equipment's interconnect the applications. As packet traverse through the network, they are queued in buffers and from time to time they are dropped due to buffer overflow.

If the drop is made intentional, detecting the correlation related to the lost packets from each hop of the path can easily identify the cause of packet loss. Hence the proposed mechanism is based on detecting the correlation of the lost packets over each hop. The correlation of lost packets is calculated as the auto-correlation function of bitmap.

The accuracy in detecting the malicious node is achieved by exploiting the correlations between the positions of lost packets. This can be calculated from the auto-correlation function (ACF) of the packet-loss bitmap. The bitmap describes the lost/received status of each packet in a sequence of consecutive packet transmissions. By detecting the correlations between lost packets, one can decide the cause of packet drop.

But the truthfulness of packet-loss bitmaps reported by individual nodes is a major challenge faced in this system. Hence auditing is required. To delegate the burden of auditing and detection homomorphic linear authenticator (HLA) cryptographic primitive is used, which is a signature scheme widely used in cloud computing and storage server systems.This development is privacy protect, scam proof and provides low communication overheads.Hence the proposed system provides high detection accuracy, the privacy-preserving feature which is attained by apublic auditor and it incurs low communication and storage overheads at intermediate nodes.

The proposed mechanism consists of 4 phases:

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. S decides a symmetric-key crypto system and k symmetric keys.Besides the symmetric key distribution, S also needs to identify the HLA keys and thusgenerating 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 (not just the key-holder) 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 every packet. These signatures are sent together along with the packet to the route by using a one-way chained encryption.

Audit Phase

Based on the information in the database explained in the previous phase, the node generates a packet-reception bit-map. Node submits these data to the auditor, as a proof of packets it has received. If the node details are similar as that of the details provided by the bit-map, the node can be considered as legitimate. If not, that particular node which holds inequality is claimed to be the malicious node.

The above mechanism can only guarantee that a node cannot understate its packet loss. The node cannot claim the reception of a packet that it did not receive a packet that it actually received.

Detection phase

Here 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.Auditor checks the consistency of the bitmaps for any possible packet loss. After checking the consistency, the auditor starts constructing the per-hop packet-loss bitmap. This is done sequentially, starting from the first hop. Only the packets lost are accounted by the auditor.

The auditor calculates the autocorrelation function for each sequence of bitmaps and then the relative differences are observed in deciding whether the packet loss is caused by malicious drop.

The HLA construction is publicly verifiable and privacy preserving. Even the auditor cannot determine the content of the packets transmitted from the PSD.

Re-routing phase

In addition, re-routing after the detection of malicious node can mitigate the effect of packet drop. Randomized dispersive routes are best effective method. Instead of selecting paths from a pre-computed set of routes, best path is chosen from the multiple paths which is selected in a randomized way As a result large number of routes can be generated for each source and destination.

Moreover, as a future work the collaborative approach of multi-hop wireless network can be used to broadcast the malicious node information to other nodes. This mechanism may increase the detection efficiency and reduce the overhead made by the auditor.

IV. Conclusion

Detecting malicious packet dropping is a crucial issue in networks. The conventional detection algorithms face several challenges that is best suited by the proposed approach. Exploiting the correlation between the lost packets improves the accuracy in detecting malicious packet drops. The truthfulness of the bitmap reported by each node is ensured by the cryptographic primitive which enables a public auditing architecture which is developed by HLA. This approach provides high detection accuracy. The randomized dispersive routes on detecting the malicious nodes effectively overcome the packet drop.

To evaluate the performance of the proposed method, we simulated it using NS2. Experimental results relieved that proposed method performs well.

Even though some open issues are to be considered in the future work. Changes in topology and link-characteristics are to be considered. In this paper we have assumed the source and destination are truthful, but malicious source and destination is a possibility which needs to be considered. The collaboration of nodes can also be exploited within the nodes to increase the efficiency of the routing path chosen. Hence a collaborative approach in detecting the malicious node based on the paper COCOWA can be applied as a future work.

References

[1]. "Robust routing in wireless Ad hoc Networks", University of Maryland, 2002
[2]. 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.
[3]. K. Balakrishnan, J. Deng, and P. K. Varshney,
[4]. "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005.
[5]. 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., vol. 6, no. 5, pp. 536–550, May 2006.
[6]. G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. Int. Conf. Theory Appl.Cryptol. Inf. Security, 2009
[7]. W. Kozma Jr. and L. Lazos, "Dealing with liars: Misbehavior identification via Renyi-Ulam games," presented at the Int. ICST Conf. Security Privacy in Commun. Networks, Athens, Greece, 2009.
[8]. W. Kozma Jr., and L. Lazos, "REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. ACM Conf. Wireless Netw. Secur., 2009

[9]. “Malicious Node detection for mobile ad hoc networks”,International Journal of computer science, vol 2, 2010

[10]. Shu.T, Krunz.M, and Liu.S, “Secure data collection in wireless sensor networks using randomized dispersive routes”. Vol. 9 no. 7, pp. 941–954, Mar 2010.

[11]. Wang.C, Wang.Q, Ren.K, and Lou.W. “Privacy-preserving public auditing for data storage security in cloud computing”, Mar. 2010.

[12]. Proano.A and Lazos.L “Packet-hiding methods for preventing selective jamming attacks” Dependable and Secure Computing., vol. 9, no. 1, pp. 101–114, Aug 2012.

[13]. Amutha.S, Balasubramanian.K, “Secure Implementation ofRouting Protocols for Wireless Ad hoc Networks” pp. 960-965, Feb 2013.

[14]. “Secure routing and attack detection in wireless ad hoc network”,vol 1, oct 2014

[15]. Tao Shu and Marwan Krunz “Privacy-Preserving and truthful Detection of packet dropping attacks in wireless ad hoc networks”, vol 14, no. 4 April 2015