Detecting Truthfulness of Packet Dropping Attacks using Public Auditing System in Wireless Ad-Hoc Networks

Monika Nag K J[1] Mr. S Lokesh[2]
[2]Associate Professor
[1]Department of PGSCEA Computer Network Engineering [2]Department of Computer Science Engineering
[1,2]The National Institute of Engineering, Mysore

Abstract— Multi-hop wireless ad-hoc network gives increased coverage and provide several benefits over traditional wireless local area networks. This architecture makes it more vulnerable to internal attacks from compromised nodes. One of them is packet dropping attack which is a crucial issue in networks. Link error and malicious packet dropping are two sources for packet losses. While observing a sequence of packet losses in the network, it is difficult to identify whether the loss is due to link errors or malicious nodes. This paper focuses on the insider-attack case, whereby malicious nodes that are part of the route selectively drop a small amount of packets which are critical to the network performance. The malicious node may identify the importance of various packets and then it drops few packets which are important to the network operation. Since packet dropping rate in this case is comparable to the channel error rate, existing detection algorithms cannot achieve satisfactory detection accuracy in identifying packet loss rate. Detection accuracy can be improved by exploiting the correlations between lost packets. In this paper, a public auditing system is used which allows the detector to verify the truthfulness of the packet loss information. The proposed mechanism is privacy preserving, collusion proof, and it incurs low communication and storage overheads at intermediate nodes. The proposed mechanism achieves better detection accuracy than the conventional methods such as a maximum-likelihood based detection.

Key words: Packet Dropping, Auditing, Attack Detection, Secure Routing

I. INTRODUCTION

In a multi-hop wireless network, nodes cooperate in relaying/routing traffic. An adversary can exploit this cooperative nature to launch attacks. For example, the adversary may first pretend to be a cooperative node in the route discovery process. Once being included in a route, the adversary starts dropping packets. 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. Eventually, such a severe Denial-of-Service (DoS) attack can paralyze the network by partitioning its topology.

There are different reasons for packet loss which is shown in fig.1. A malicious node that is part of the route can exploit its knowledge of the network protocol and the communication context to launch an insider attack–an attack that is intermittent, but can achieve the same performance degradation effect as a persistent attack at a much lower risk of being detected. Specifically, the malicious node may evaluate the importance of various packets, and then drop the small amounts that are deemed highly critical to the operation of the network. For example, in a frequency-hopping network, these could be the packets that convey frequency hopping sequences for network-wide frequency-hopping synchronization; in an ad hoc cognitive radio network, they could be the packets that carry the idle channel lists (i.e., white spaces) that are used to establish a network-wide control channel. By targeting these highly critical packets, intermittent insider attacker can cause significant damage to the network with low probability of being caught. In this paper, we are interested in combating such an insider attack. In particular, we are interested in the problem of detecting the occurrence of selective packet drops and identifying the malicious node(s) responsible for these drops.

In this paper, we develop an accurate algorithm for detecting selective packet drops made by insider attackers. Our algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision.

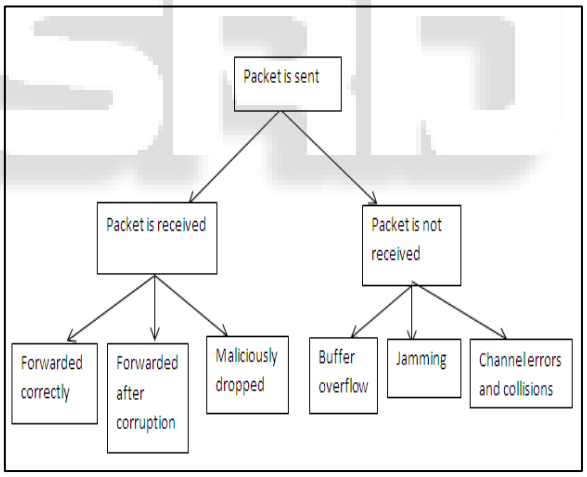

Fig. 1: Overview of Packet Loss

A. *Problem Statement:*

Detecting selective packet-dropping attacks is extremely challenging in a highly dynamic wireless environment. The difficulty comes from the requirement that we need to not only detect the place where the packet is dropped, but also identify whether the drop is intentional or unintentional. Specifically, due to the open nature of wireless medium, a packet drop in the network could be caused by rough channel conditions (e.g., fading, noise, and interference, link errors), or by the insider attacker. In an open wireless environment, link errors are quite significant, and may not be significantly smaller than the packet dropping rate of the insider attacker. We require the detection to be performed by the public auditor that does not have knowledge of the data held by the nodes on the network route. When a

malicious node is identified, the auditor should be able to construct a proof of the misbehavior of that node.

II. RELATED WORK

The related work on the detection of packet dropping attacks can be classified into two categories.

A. The first category aims at high malicious dropping rates, where most (or all) lost packets are caused by malicious dropping. In this case, the impact of link errors is ignored.

Most related work falls into this category. Based on the methodology used to identify the attacking nodes, these works can be further classified into four sub-categories. The first sub-category is based on credit systems. A credit system provides an incentive for cooperation. A node receives credit by relaying packets for others, and uses its credit to send its own packets. As a result, a maliciously node that continuous to drop packets will eventually deplete its credit, and will not be able to send its own traffic. The second sub-category is based on reputation systems. A reputation system relies on neighbors to monitor and identify misbehaving nodes. A node with a high packet dropping rate is given a bad reputation by its neighbors. This reputation information is propagated periodically throughout the network and is used as an important metric in selecting routes. Consequently, a malicious node will be excluded from any route. The third sub-category of works relies on end-to-end or hop-to-hop acknowledgements to directly locate the hops where packets are lost. A hop of high packet loss rate will be excluded from the route.

B. The second category aims at the scenario where the number of maliciously dropped packets is higher than that caused by link errors, but the influence of link errors is non-negligible.

A. Disadvantages:

1) For the credit-system-based method, a malicious node may still receive enough credits by relaying most of the packets it receives from upstream nodes.
2) In the reputation-based approach, the malicious node can maintain a reasonably good reputation by forwarding most of the packets to the next hop.
3) For the acknowledgement-based method and all the mechanisms in the second category, counting the number of lost packets does not give a sufficient ground to detect the real attacker that is causing packet losses.

III. PROPOSED SYSTEM

The proposed method is based on detecting the correlations between the lost packets over each hop of the path. It provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) which describes the status of each packet in a sequence of packet transmission. Therefore, by detecting the correlations between the lost packet, one can decide whether the packet loss is purely due to link errors, or is a combined effect of malicious drop and link error.

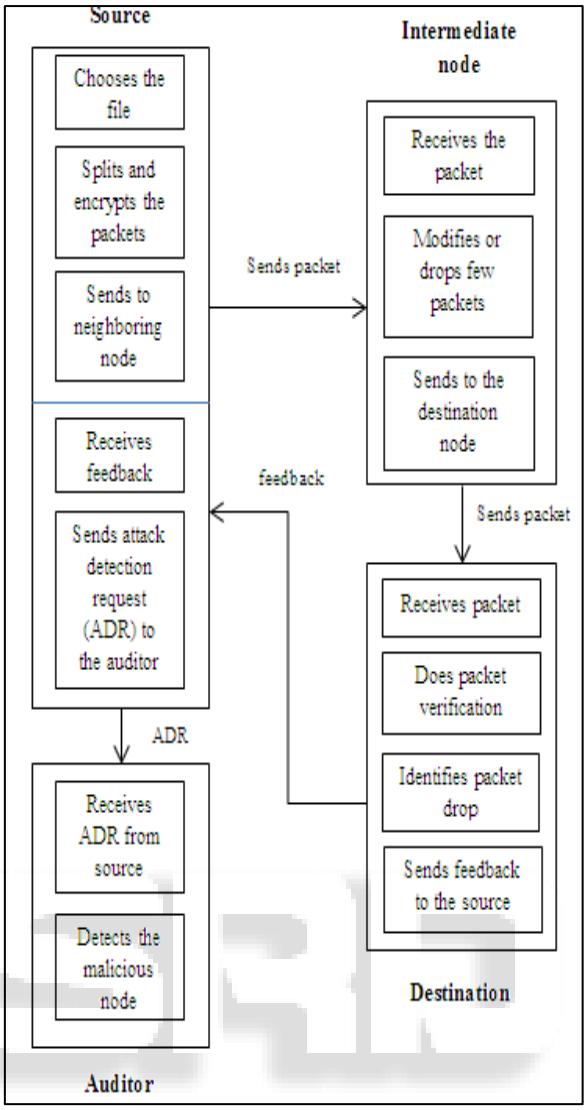

Fig. 2: Proposed Architecture

A. Network Model:

The wireless channel as shown in figure 3., in which the source node continuously sends packets to the destination node through intermediate nodes $n_{1.....}n_k$ (where n_i is the upstream node of n_{i+1}). is modeled of each hop along P (Path to Source and Destination) as a random process that alternates between good and bad states. Packets transmitted during the good state are successful, and packets transmitted during the bad state are lost. A sequence of M packets is transmitted over the channel.

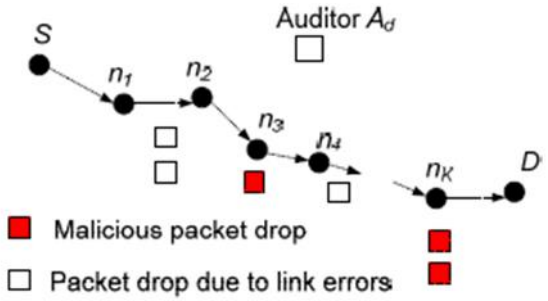

Fig. 3: Network and Attack Model

B. Independent Auditor:

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

C. Setup Phase:

This phase takes place right after path P is established, but before 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.

D. Advantages of Proposed System:

1) High detection accuracy.
2) Privacy preserving.
3) Low communication and storage overheads.

IV. CONCLUSION

It is compared with conventional detection algorithms that utilize only the distribution of the number of lost packets, exploiting the correlation between lost packets significantly improves the accuracy in detecting malicious packet drops. Such improvement is especially visible when the number of maliciously dropped packets is comparable with those caused by link errors. To correctly calculate the correlation between lost packets, it is critical to acquire truthful packet-loss information at individual nodes. Developed Public auditing architecture ensures truthful packet-loss reporting by individual nodes. This architecture is collusion proof, requires relatively high computational capacity at the source node, but incurs low communication and storage overheads over the route.

REFERENCES

[1] A. Proano and L. Lazos. Packet-hiding methods for preventing selective jamming attacks. IEEE Transactions on Dependable and Secure Computing, 9(1):101–114, 2012.
[2] T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim. Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks. In Proceedings of the IEEE ICC Conference, 2009.
[3] M. Kiran kumar and A. Sai harish. A novel schema for detecting malicious packet losses. International journal of modern engineering research, 2012.
[4] A. Proano and L. Lazos. Selective jamming attacks in wireless networks. In Proceedings of the IEEE ICC Conference, pages 1–6, 2010.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou. Privacy-preserving public auditing for data storage security in cloud computing. In Proceedings of the IEEE INFOCOM Conference, Mar. 2010.
[6] M. Just, E. Kranakis, and T. Wan, ―Resisting malicious packet dropping in wireless ad hoc networks,in In Proc. of ADHOCNOW03. Springer Verlag, 2003, pp. 151–163.
[7] F. Anjum and R. Talpade, ―Lipad: lightweight packet drop detection for ad hoc networks,‖ Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, vol. 2, pp. 1233–1237 Vol. 2, Sept. 2004
[8] O. F. Gonzalez, M. P. Howarth, and G. Pavlou, ―Detection of packet forwarding misbehavior in mobile ad-hoc networks.‖ in WWIC,ser. Lecture Notes in Computer Science, F. Boavida, E. Monteiro,

