International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 3: March 2016, pp 1-3. www.aetsjournal.com ISSN (Online) : 2394-6237

A Survey on Packet Dropping Attacks in Wireless Ad Hoc Networks

K.Thenmozhi, G.Sudhakar

Abstract— In this paper we discuss about various packet dropping attacks in wireless Ad Hoc networks. In particular we discuss about the sequence of packet losses in the network whether the losses are caused by the losses are caused by link errors only, or by the combined effect of link errors and malicious drop. A lots of papers are taken for the survey and its advantages and disadvantages are discussed below

Keywords— Packet drop attacks, Packet loss, Malicious drop

I. INTRODUCTION

In computer networking, a packet drop attack or blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool.[1] 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. The packet drop attack can be frequently deployed to attack wireless ad hoc networks. Because wireless networks have a much different architecture than that of a typical wired network, a host can broadcast that it has the shortest path towards a destination.

Hybrid wireless networks are networks in which any mobile node in a wireless network may have connectivity, either directly or via a gateway node, to an infrastructure network. This latter network may be an IP network as the Internet, a 3G wide area wireless network, or an 802.11 local area wireless network. [4]Actually, any other network technology may be considered. In this context, the notion of Intra technology and Inter technology appears. If a mobile node communicates with another network of similar technology, this can be seen as Intra technology hybrid wireless network. As for example, the case of a mobile node in an ad hoc 802.11 network communicating with an 802.11 Access Point (AP) in an infrastructure network. On the other hand, if a mobile node communicates with another network of different technology, this can be seen as Inter technology hybrid wireless network. For example, the case of a mobile node in an 802.11 network communicating with a 3G network. Moreover, hybrid wireless networks may integrate both Intra and Inter technology cases and the mobile node itself may support heterogeneous technologies switching between them in an on-demand fashion

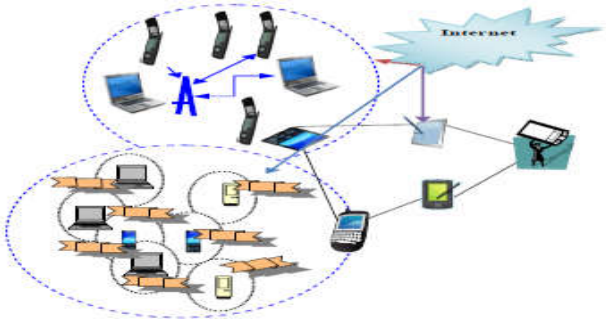

Fig 1 Hybrid Wireless Network

In the above fig 1 it describes about the hybrid wireless network in which all nodes are connected. These special nodes are having limited processing and communication capability due to limited energy

II. IMPORTANT TECHNIQUES

In a multi-hop wireless ad hoc network, packet losses are attributed to harsh channel conditions and intentional packet discard by malicious nodes. In this paper, while observing a sequence of packet losses, we are interested in determining whether losses are due to link errors only, or due to the combined effect of link errors and malicious drop. We are especially interested in insider's attacks, whereby a malicious node that is part of the route exploits its knowledge of the communication context to selectively drop a small number of packets that are critical to network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, we propose to exploit the correlations between lost packets.

- *Network Modeling*

The wireless channel is modeled of each hop along PSD (Path to Source and Destination) as a random process that alternates between good and bad states. Packets transmitted

K.Thenmozhi, PG scholar, Department of Computer Science and Engineering, Ranganathan Engineering college, Coimbatore, Tamilnadu, India. (Email: thenmozhircse46@gmail.com)

G.Sudhakar, Assistant Professor, Department of Computer Science and Engineering, Ranganathan engineering college, Coimbatore, Tamilnadu, India. (Email: Sudhakar.g7018@gmail.com)

during the good state are successful, and packets transmitted during the bad state are lost

- *Independent Auditing*

There is an independent auditor Ad in the network. Ad is independent in the sense that it is not associated with any node in PSD. 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

- *Packet Drop Detection*

The proposed mechanism is based on detecting the correlations between the lost packets over each hop of the path. The basic idea is to model the packet loss process of a hop as a random process alternating between 0(loss) and 1 (no loss)

- *Set Up Phase*

This phase takes place right after route PSD is established,but before any data packets are transmitted over the route. In this phase, S decides encrypt the packets and sent through the route to destination

Table 1
Analysis Of Packet Dropping Attacks

S.NO	TITLE	DESCRIPTION
1	802.11 Markov channel modeling[1]	Wireless fading channels are commonly characterized by Markov models. Almost all models assume the underlying channel has flat fading characteristics and that fairly simply modulation schemes are used
2	Provable data possession at untrusted stores[2]	In this we introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it
3	Proofs of storage from homomorphic identification protocols[3]	Proofs of storage (PoS) are interactive protocols allowing a client to verify that a server faithfully stores a file. Previous work has shown that proofs of storage can be constructed from any homomorphic linear authenticator (HLA)
4	ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks[4]	Ad hoc networks offer increased coverage by using multi-hop communication. This architecture makes services more vulnerable to internal attacks coming from compromised nodes that behave arbitrarily to disrupt the network, also referred to as Byzantine attacks
5	TWOACK: Preventing selfishness in mobile ad hoc networks[5]	Mobile Ad hoc Networks (MANETs) operate on the basic underlying assumption that all participating nodes fully collaborate in self-organizing functions
6	Short signatures from the weil pairing[6]	In this we introduce a short signature scheme based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves
7	Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)[7]	Mobile ad-hoc networking works properly only if the participating nodes cooperate in routing and forwarding.
8	Stimulating cooperation in self organizing mobile ad hoc networks[8]	In this paper, we consider the case when each node is its own authority and tries to maximize the benefits it gets from the network
9	Modelling incentives for collaboration in mobile ad hoc networks[9]	This paper explores a model for the operation of an ad hoc mobile network. The model incorporates incentives for users to act as transit nodes on multi-hop paths and to be rewarded with their own ability to send traf
10	Routing amid colluding attackers[10]	In this we propose the first practical solution to the long-routing layer attacks, and provides good performance in be standing problem of secure wireless routing in the presence nign conditions. .

III. CONCLUSION

In this paper we discuss about various packet drop attacks in wireless Ad hoc networks to prevent the datas and for privacy purpose. The result of these techniques are being analysed. The result shows that "Proofs of storage from homomorphic identification protocols," gives a better outcome when compared to other techniques

REFERENCES

[1] J. N. Arauz, "802.11 Markov channel modeling," Ph.D. dissertation,School Inform. Sci., Univ. Pittsburgh, Pittsburgh, PA, USA, 2004

[2] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable data possession at untrustedstores," in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007, pp. 598–610.

[3] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphicidentification protocols," in Proc. Int. Conf. Theory Appl.Cryptol. Inf. Security, 2009, pp. 319–333.
[4] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008
[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, pp. 2137–2142.
[6] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," J. Cryptol., vol. 17, no. 4, pp. 297–319, Sep. 2004
[7] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf., 2002, pp. 226–236
[8] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in selforganizingmobile ad hoc networks," ACM/Kluwer Mobile Netw.Appl., vol. 8, no. 5, pp. 579–592, Oct. 2003.
[9] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," presented at the First Workshop Modeling Optimization Mobile, Ad Hoc Wireless Netw., Sophia Antipolis, France, 2003
[10] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "Routing amidcolluding attackers," in Proc. IEEE Int. Conf. Netw. Protocols, 2007,pp. 184–193.