DISCLOSURE OF PACKET DROPPING ATTACKS IN WIRELESS AD HOC NETWORKS

GADHAMSETTY PRASANTH
Asst.Prof in CSE Dept,
Avanthi's Scientific Technological
and Reseach Academy, Hyderabad

PR PRASAD
Asst.Prof in CSE Dept,
Avanthi's Scientific Technological
and Reseach Academy, Hyderabad

ABSTRACT

In wireless ad hoc network, Denial-of-service (DoS) attacks can deplete network resources and energy externally much effort on the part of an opponent, where Packet was dropping advances are one category of DoS attacks consequently packet loss is a serious issue. In our presented system scenario, the malicious nodes in a route can purposely drop the packets through the diffusion from a source toa destination either it is caused by link errors or by malicious packet dropping.It is hard to diverge the packet loss caused by link errors and malicious dropping more over for identifying such attacks in ad hoc networks every node should monitor in the system. When they detect malicious nodes that fall packets, a new path has to find that it does not include them in a communicated network.In this paper, we are exploring a new solution called AP-HLA(Alternative path-homomorphic linear authentication) it isolates the paths that drop packets via alternative paths that WSN finds so far during route discovery. As a result, it leads packet-dropping attack acquires no additional cost because one of the alternate paths utilized for all subsequent communication, hence to improve the detection accuracy, the correlations between lost packets identified. In our proposed approach monitoring individual nodes are not required, which determines the malicious packet dropping by the correlation among packets. Similarly, an auditing architecture based on homomorphic linear authenticator can be used to confirm the proof of reception of packets at each node.

Keywords: *ad-hoc wireless network, Denial-of-service (DoS) attacks, Alternative path-homomorphic linear authentication*

1. INTRODUCTION

WSNs are typically reactive, and the wireless medium naturally broadcasts in nature. It marks WSNs exposed to all classes of denial-of-service (DoS) attacks. In a wireless ad hoc network, nodes broadcast with respectively other via wireless links either directly or relying on other nodes as routers. Without proper security measures, an adversary can blastoff various kinds of attacks in hostile environments.DoS attacks (like packet dropping, false route request, or flooding) an deplete the network of energy without much trouble on the part of an adversary.

An adversary may misbehave by supportive to forward packets and then failing to do so. When being included in a route, the adversary starts dropping packets. That means it stops forwarding the packet to the next node. The malicious node can exploit its consciousness about the protocol to perform an insider attack. It can analyze the importance of the transmitting packet and can select drop those packets. Hence, it can completely control the performance of the network. If the attacker is continuously dropping packages, it can discover and mitigate efficiently. Since even if the malicious node is unidentified, one can use the randomized, multi-path routing algorithms to avoid the black holes generated by the attack. If the malicious nodes get identified, the node can remove from the routing table of the network. The discovery of discriminatory packet dropping is robust. Occasionally the dropping of packets may not be deliberate. It can occur as a result of channel errors. So the detection mechanism should be capable of differentiating the malicious packet dropping and the dropping due to link errors.

Our proposed solution efficiently works to identify the selective packet dropping. It increases the detection accuracy by computing the correlation between lost packets with the help of an Auto-Correlation Function of the bitmaps at each node in the route To improve the detection accuracy, the correlations between lost packets identified.

2. RELATED WORK

Vijay Bhuse et al.,[1] discussed new techniques for detection of packet-dropping nodes in ad hoc networks author propose a lightweight solution called DPDSN. It identifies paths that drop packets by using alternate paths that WSN finds earlier during route discovery. Responding to a packet-dropping attack incurs no additional cost because one of the alternate paths is utilized for all subsequent communication.

Cao Shu et al.,[2] author targets the challenging situation where link errors and malicious dropping lead to comparable packet loss rates. The effort in the literature on this problem has been quite preliminary, and there are a few related works. Note that the cryptographic methods proposed in [3] to counter, particular packet jamming target a different issue than the detection problem studied in this paper. The methods in [3] delay a jammer from recognizing the significance of a packet after the packet has been successfully transmitted so that there is no time for the jammer to conduct jamming based on the content/importance of the packet. Instead of trying to detect any maliciousbehaviour, the approach in [3] is proactive, and hence incurs overheads regardless of the presence or absence of attackers.

3. PROPOSED SYSTEM MODEL:

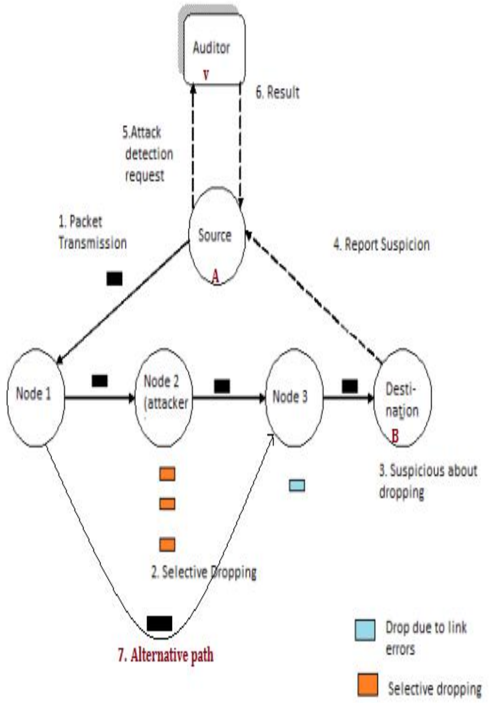

Fig 1. System Model

In our system model Let P_{AB} be an arbitrary route in an ad-hoc wireless network. The source is aware of the path, and it sends packets continuously to the destination B through P_{AB}. Consider that the network is quasistatic type means the network topology and link characteristics are constant for a relatively extended period. Each hop that constitutes the path alternates between good and bad states. Packets transmitted during the good state, are successful, and packets sent during the bad state lost. By observing whether the transmissions are successful or not, the receiver obtains a realization of the channel state, which is a combination of zeros and ones. In that "1" denotes the packet successfully received, and "0" denotes the packet dropped. When the receiver notifies some suspicious packet loss, it reports feedback to the sender. The detection of malicious dropping is performed by a self-governing auditor A. After receiving the response from the receiver; the sender requests the auditor to perform the detection. The auditor module identifies the malicious dropping by checking the correlation between lost packets at each node. The correlation between lost packet in particular dropping condition and link error condition is different [2]. For this, the information collected by the auditor will be accurate. To ensure that the packet received by a node, the mechanism proposed here uses a homomorphic linear authenticator. Also, to ensure the packet forwarding, it uses the alternative Path-based mechanism to forward the packet without delay.

PROBLEM STATEMENT

The adversary, a node affected in the path, it may try to degrade the performance of the system by dropping the packets sent by the source. The node can perform the dropping selectively or randomly. The detection should be done by an independent auditor module. While performing detection, it should verify the correctness of collecting information. Also, should produce publicly verifiable proof of the misbehaviour of the node. Besides this, there is a chance of collision between two nodes. A covert communication channel may exist between any two malicious nodes, in addition to the path connecting them on P_{SD}. As a result, malicious nodes can exchange any information without being detected by Ad or any other nodes in P_{SD}. Malicious nodes can take advantage of this covert channel to hide their misbehaviour and reduce the chance of being detected.

DETECTION OF PACKET DROPPING:

In this section, the discoverypatternattentionsthe correlation among the lost packets at for each node in the transmission route. Though the sender A transmitting the packets consecutively, each hop in the path will retain a transmission bitmap for every packet. The bitmap is a pattern of 0 and 1, where 1signifies the successfully transmitted packet, and 0 signifies the unsuccessfully transmitted packets. By an Auto-Correlation Function (ACF), the correlation between these bitmaps can calculate. In various packet dropping circumstances, the correlation function will generate different values. Therefore, by observing the correlations between lost packets, one can select whether the packet loss is purely due to regular link errors, or is a collective effect of link error and malicious drop.

However, the principalexperiment is that the packet-loss bitmaps reported by individual nodes along the route may not be correct. For the proper calculation of the correlation between lost packets, the truthfulness of bitmap is necessary. Auditing functionality can achieve this. Auditing can do by using a cryptographic primitive called homomorphic linear authenticator (HLA), which is a signature scheme to provide a proof of storage from the server assigning clients in cloud computing and stockpiling server systems. Besides this, to ensure the forwarding, a reputation-based mechanism can be used. When a node relays the packet, effectively, it gets a good reputation from the receiving node. That means, in a path from sender to receiver, the node with a minimum reputation dropped more packets.

4. PROPOSED SYSTEM DESIGN

The system consists of four Phases:

i. Setup Phase
ii. Packet Transmission Phase
iii. Audit Phase
iv. Detection Phase
v. Alternative path

Setup Phase:

Straight away after launching the route, the configuration phase gets started. The source elects on the symmetric key cryptosystem for encryption the packet throughout the transmission phase. Source securely distributes a decryption key and a symmetric key to each node on the path. Key distribution may base on thepublickeycryptosystem. The source also announces two hash functions to every node in the route. Besides this, the source also needs to set up its HLA keys.

Packet Transmission Phase:

After the successful completion of Setup phase, source enters into the transmission phase. In this phase, before the transmission of a packet's source computes the hash value of each packet, and generates HLA signatures of the hash value for each node. These signatures are then sent composed with the packets to the routerthruby one-way sound encryption. This prevents the deciphering of the signatures for downstream nodes by the upstream node. When a node in the route has received the packet from the source, it extracts packets and signature. Then it verifies the integrity of the expected packet. A database continued at each node on P_{SD}. It can measure as a FIFO queue which records the reception status for the packets sent by the source. Each node stores the received hash value, then signature in the database as proof of reception.

Audit Phase

In audit phase when the source issues an attack detection request, the audit phase gets started. The ADR message includes the id of the nodes on the route, source' s HLA public key information, the sequence numbers of the packets sent by the source, and the sequence numbers packets that were received by the destination. The auditor requests the packet bitmap information from each node in the route by issuing a challenge. From the information stored in the database, every node generates this bitmap. The Auditor checks the validity of bitmaps and accepts if it is valid. Otherwise, it rejects the bitmap and considers the node as a wicked one. This mechanism only guarantees that a node cannot understate its packet loss, i.e., it cannot claim the reception of a packet that it did not receive. This mechanism cannot prevent a node from overly stating its packet loss by arguing that it not receive a packet that it received. This latter case is limited by the mechanism based on reputation which is discussed in the detection phase.

Identification or detection Phase

After auditing the response to the challenge provided by the auditor, it arrives into the discovery phase. Auditor makes per hop bitmaps, and by using an autocorrelation function (ACF), it will find out the relationship between the lost packets. Then it finds out the difference between the calculated value and correlation value of the wireless channel. Based on the relative difference, it decides whether the packet loss is due to the malicious node or link errors. When it finds out the malicious drop, it can consider both ends of the hop as suspicious. That means either the transmitter did not send the packet, or receiver did not receive. After identifying these two suspicious nodes, the detector needs to find out the actual attacker. For this, it can check the reputation value. Now the Auditor module will collect the reputation value of the two suspicious nodes. When a node fails to forward the packet, it will get a minimum reputation. By checking this, the detector can easily distinguish the attacker.

Alternative path:

When adversary node is identified by the auditor module to identify the malicious dropping by checking the correlation between lost packets at each node.Thus, there may be a chance of data loss or modified at the affected node, to provide the data transmission in identifying adversary node network, data will be forwarded through an alternative path which transmitted to its successive node and finally,reaches the destination.Adversary node will heal by the source through a replica mechanism.

5. CONCLUSION

In this paper,to identify the malicious node that drops the packets deliberately, the technique definednowutilizes the correlation between the lost packets at each node in the route from source to destination. AP-HLA is a proposed mechanism will give a satisfactory improvement in the detection accuracy ofparticularpacket dropping towards correctly calculate the correlation between lost packets, it requires accurate packet loss information from every node in the route.The Auditor ensures the integrity of packet loss information of each node by using Homomorphic Linear Authenticator (HLA). AP-HLA-based public auditing architecture ensures accurate packet-loss reporting by the various nodes. This architecture is collusion-proof, requires a comparativelyextraordinaryour proposed approach monitoring individual nodes are not required, which determines the malicious packet dropping by the correlation among packets. Similarly, an auditing architecture based on homomorphic linear authenticator can be used to confirm the proof of reception of packets at each node.

REFERENCES

[1].*Sneha C.S and Bonia Jose," DETECTING PACKET DROPPING ATTACK IN WIRELESS AD-HOT NETWORK", International Journal on Cybernetics & Informatics (IJCI) Vol. 5, No. 2, April 2016*

[2]. *Tao Shu and Marwan Krunz," Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 4, APRIL 2015, Digital Object Identifier no. 10.1109/TMC.2014.2330818*

[3]. *A. Proano and L. Lazos, "Selective jamming attacks in wireless networks," in Proc. IEEE ICC Conf., 2010, pp. 1–6.*

[4] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable securerouting for ad hoc networks," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 –9.

[5] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation-based incentive scheme for ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2004, pp. 825–830.

[6] 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.

[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.