ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Detection of Malicious Packet Dropping in Wireless Ad Hoc Networks Based on Privacy-Preserving Public Auditing

Bhagyashree S.[1], Prof. Anand S Uppar[2]

Department of Computer Science and Engineering, Shree Devi Institute of Technology, Mangalore, India[1]

HOD, Department of Computer Science and Engineering, Shree Devi Institute of Technology, Mangalore, India[2]

Abstract: Security is one of the most important issues that have attracted a lot of research and development effort in past few years. In multi-hop wireless ad hoc network link error and malicious packet dropping are two sources for packet losses. Whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop are to be identified, can be known by observing a sequence of packet losses in the network. But in the insider-attack case, whereby malicious nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance. Conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy because the packet dropping rate in this case is comparable to the channel error rate. Hence to improve the detection accuracy, the correlations between lost packets is identified. The technique called Homomorphic linear authenticator (HLA) based public auditing architecture is developed that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This technique provides privacy preserving, collusion proof, and incurs low communication and storage overheads. A packet-block based mechanism is also proposed, to reduce the computation overhead of the baseline scheme, which allows one to trade detection accuracy for lower computation complexity.

Keywords: Homomorphic linear authenticator, Auditing, AES.

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 server 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. Even though persistent packet dropping can effectively degrade the performance of the network, from the attacker's standpoint such an "always-on" attack has its disadvantages.

To find this type of packet dropping there is many types of technique proposed .There are two type of classification in the technique. 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. Crediting system, Reputation system, End-to-end or hop-to-hop [3] acknowledgements and Cryptographic methods [4] . A credit system [1] 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. A reputation system [2] 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. Bloom filters used to construct proofs for the forwarding of packets at each node. By examining the relayed packets at successive hops along a route, one can identify suspicious hops that exhibit high packet loss rates. The second category [5] targets the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible.

II. LITERATURE SURVEY

In the year 2003 Borzoo Shadpour, Shahrokh Valaee, Baochun Li proposed paper titled "A Self-Organized Approach for Stimulating Cooperation in Mobile Ad Hoc Network" which contain the self-organized mechanism

DOI 10.17148/IJIREEICE

that is broke service, which allows for a broke node to use the network to transmit its traffic, in addition it providing an incentive to stimulate non-broke nodes to cooperate with broke ones. The main idea is to improve the connectivity of broke nodes in a pure ad-hoc networks. The proposed solution is loaning, which is interesting since it can be performed 'on-the-fly' by the nodes systems, and is suitable for the conditions of ad-hoc networks since it allows for nodes to remain self-organized. This scheme stimulates nodes to actively participate in the network, allowing the broke nodes to experience less delay when urgent transmission is desired.

In the year 2005 Wenyuan XU, Wade Trappe, Yanyoung Zhang, Timothy Wood proposed a paper titled "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Network" which examine radio interference attacks from both sides of the issue: first, study the problem of conducting radio interference attacks on wireless networks, and second examine the critical issue of diagnosing the presence of jamming attacks. Specifically, proposes four different jamming attack models that can be used by an adversary to disable the operation of a wireless network, and evaluate their effectiveness in terms of how each method affects the ability of a wireless node to send and receive packets. The paper also study different measurements that serve as the basis for detecting a jamming attack, and explore scenarios where each measurement by itself is not enough to reliably classify the presence of a jamming attack. In particular the signal strength and carrier sensing time are unable to conclusively detect the presence of a jammer. The paper proposes two enhanced detection protocols that employ consistency checking. The first scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, while the second scheme employs location information to serve as the consistency check. In the paper the feasibility and effectiveness of jamming attacks and detection schemes using the MICA2 Mote platform.

In the year 2007 Jakob Erikson, Michalis Faloutsos, Srikanth V, Krishnamurthy proposed a paper titled "Routing amid Colluding Attackers "with the first practical solution to the long-standing problem of secure wireless routing in the presence of colluding attackers. The secure routing protocol, Sprout1, continuously tries new routes to the destination. Routes are generated probabilistically, with complete disregard for performance metrics. This nature makes Sprout uniquely resilient to attack. it cannot be tempted by any kinds of shortcuts. To avoid compromised routes, and to ensure good overall performance, the quality of each active route is monitored by means of signed end-to-end acknowledgments. Based on this end-to-end acknowledgments amount of traffic sent on each route is adjusted accordingly. The vast majority of known routing layer attacks is mitigated by Sprout effectively, even when under assault from a large number of colluding attackers. . Sprout consistently delivers high, reliable performance in benign as well as hostile environments.

In the year 2009 William Kozma Jr , Loukas Lazos proposed a paper titled "REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Network based on Random Audits" the paper investigate the problem of uniquely identifying the set of misbehaving nodes who refuse to forward packets. The resource-efficient account- ability for node misbehavior is identified by the new misbehavior identification scheme called REAct. The identification of misbehaving nodes based on a series of random audits triggered upon a performance drop is done in REAct. The source-destination pair using REAct can identify any number of independently misbehaving nodes based on behavioral proofs provided by nodes. Proofs are constructed using Bloom filters which are storage efficient membership structures, thus significantly reducing the communication overhead for misbehavior detection. REAct has three phases (a) the audit phase (b) the search phase (c) the identification phase.

In the year 2010 Divya Ann Luke, Dr Jayasundha. J .s proposed a paper titled "Selective Jamming Attack Prevention Based on Packet Hiding Methods and Wormholes" contain a new method to prevent the selective jamming attack in a internal thread model. The wormhole is which will generate an alarm to indicate the presence of jammer and sent IP address of jammer node to all other nodes in the network is used. We can send message through the network even though a jammer is present by sing a method called packet hiding. The technique called Strong Hiding Commitment Scheme (SHCS) this method is used. Here, the wormhole becomes the access point in a network region whenever it finds out any node that violates the rules in a particular network region. Such node is then considered as a jammer node. Wormhole sends IP address of jammer to all other nodes. The prevention of the jamming activity of the jammer is done by Wormhole, by encrypting the source ID of message along with the message packet. By doing so jammer is unable to identify its target node and the source can forward its message safely through jammer node itself.

In the year 2013 Mrs.K.Gomathy, Mr.P.Dineshkumar proposed a paper titled" Detection of Routing Misbehavior in Manet by Enhanced 2ack Scheme Using Dsr Protocol "which focuses on routing misbehavior in MANET and method for detection of misbehavior which is caused by links. All the interested nodes to participate in routing should be fully co operative in MANET. But some nodes get benefits for other nodes refuse to share their resources. Performance of network gets affected due to the node mobility, open structure and dynamic topology changes. To detect such behavior by sending acknowledgement through opposite direction of the routing path the 2ACK scheme is used. The proposed enhanced scheme using DSR protocol reduces the overhead of acknowledgement

DOI 10.17148/IJIREEICE

by 2ACK scheme. There are three modules in 2ACK system.

III. SYSTEM MODULES AND PROBLEM STATEMENTS

A. *Problem statements*

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 (or hop) 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 harsh 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. So, the insider attacker can camouflage under the background of harsh channel conditions. In this case, just by observing the packet loss rate is not enough to accurately identify the exact cause of a packet loss.

B. *System Modules:*

The system contains four modules.

1) Network modeling.
2) Independent auditing.
3) Setup phase.
4) Packet dropping detection

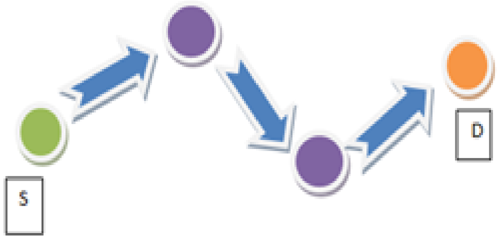

Fig1. Intermediate nodes with source and destination

1. Network modeling

The wireless channel is modeled of each hop along P_{SD} (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. It is assumed quasi-static networks, whereby the path P_{SD} remains unchanged for a relatively long time.

Detecting malicious packet drops may not be a concern for highly mobile networks, because the fast-changing topology of such networks makes route disruption the dominant cause for packet losses. In this case, maintaining stable connectivity between nodes is a greater concern than detecting malicious nodes. A sequence of M packets is transmitted consecutively over the channel.

2. Independent auditor:

There is an independent auditor Ad in the network. Ad is independent in the sense that it is not associated with any node in P_{SD}. 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. Once the destination click on verify, the action takes places to identify the packet loss. To facilitate its investigation, Ad needs to collect certain information from the nodes on route P_{SD}.

3. Setup phase

This phase takes place right after route P_{SD} 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. Destination after receiving packets can verify the packet and after verification it can decrypt the packets.

4. 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). Specifically, consider that a sequence of M packets that are transmitted consecutively over a wireless channel. Under different packet dropping conditions, packet loss is identified.

IV. SYSTEM ARCHITECTURE

To develop an accurate algorithm for detecting selective packet drops made by insider attackers. This algorithm also 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) of the packet-loss bitmap–a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions. By detecting the correlations between lost packets, one can decide whether the packet loss is purely due to regular link errors, or is a combined effect of link error and malicious drop. The main challenge in our mechanism lies in how to guarantee that the packet-loss bitmaps reported by individual nodes along the route are truthful, i.e., reflects the actual status of each packet transmission. Such truthfulness is essential for correct calculation of the correlation between lost packets; this can be achieved by some auditing. Considering that a typical wireless device is resource-constrained, we also require that a user should be able to delegate the burden of auditing and detection to some public server to save its own resources.

Public-auditing problem is constructed based on the homomorphism linear authenticator (HLA) cryptographic primitive, which is basically a signature scheme widely used in cloud computing and storage server systems to

DOI 10.17148/IJIREEICE

provide a proof of storage from the server to entrusting clients

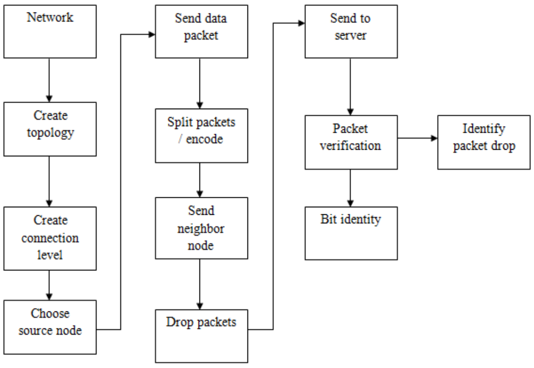

Fig2: System architecture

V. SYSTEM IMPLEMENTATION AND RESULT ANALYSIS

The system is implemented. The initially the network is configured with calling the Node configure function with number of nodes. And then Link create will create link, while creating link we need to specify the levels with which the node is associated. Once the network is configured we take up server as the destination and any of the nodes as the sender. Once the network is set we browse for the file we need to send. In the source we split the entire file in to number of packets these packets will be encrypted and Addbit function will help in adding bits to identify the change in number of packets and packet will be forwarded further. The packet will be received by the intermediated node in normal transition packet will be encrypted and forwarded whereas in attacker mode packet will be dropped or modified or both will be done and forwarded. Once the packet reach destination in normal node packet will be verified, bit identified, decrypted and finally merged. In attacker mode when packet is verified the packet dropped is identified, bit identification will let us know about packet modification. On modification or dropped packet cannot be decrypted.

We also have option for categorization which gives the number of packet received properly and number of packet modified. Also provide ranking about the node which help in routing in further packet transfer. The expected results are if any packets are modified or dropped our system has to identify the attack and the node in which the attack has occurred. This has been achieved thus gives us the proper results for the system implemented. In the system implement. We can verify the packet received and rate about the nodes participated in transmission of the packets to destination.

VI. 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. HLA-based public auditing architecture developed that 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. To reduce the computation overhead of the baseline construction, a packet-block-based mechanism was also proposed, which allows one to trade detection accuracy for lower computation complexity.Some open issues remain to be explored in our future work. First, the proposed mechanisms are limited to static or quasi-static wireless ad hoc networks. Frequent changes on topology and link characteristics have not been considered. Extension to highly mobile environment will be studied in our future work. Misbehaving source and destination will be pursued in our future research. Moreover, in this paper, as a proof of concept, we mainly focused on showing the feasibility of the proposed cypto-primitives and how second-order statistics of packet loss can be utilized to improve detection accuracy. As a first step in this direction, our analysis mainly emphasize the fundamental features of the problem, such as the untruthfulness nature of the attackers, the public verifiability of proofs, the privacy preserving requirement for the auditing process, and the randomness of wireless channels and packet losses, but ignore the particular behavior of various protocols that may be used at different layers of the protocol stack. The implementation and optimization of the proposed mechanism under various particular protocols will be considered in future studies.

REFERENCES

[1]. L. Buttyan and J. P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applica- tions, 8(5):579–592, Oct. 2003.

[2]. J. Eriksson, M. Faloutsos, and S. Krishnamurthy. Routing amid colluding attackers. 2007.

[3]. W. Kozma Jr. and L. Lazos. REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits. In Proceedings of the ACM Conference on Wireless Network Security (WiSec), 2009.

[4]. D. B. Johnson, D. A. Maltz, and J. Broch. DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks. Chapter 5, Ad Hoc Networking, Addison-Wesley, pages 139–172, 2001..

[5]. W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the ACM MobiHoc Conference, pages 46–57, 2005.

[6]. A. Proano and L. Lazos. Selective jamming attacks in wireless networks. In Proceedings of the IEEE ICC Conference, pages 1–6, 2010.

[7]. G. Noubir and G. Lin. Low-power DoS attacks in data wireles lans and countermeasures. ACM SIGMOBILE Mobile Computing and Communications Review, 7(3):29–30, July 2003.

[8]. Tao Shu and Marwan Krunz. Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks, IEEE Transactions on Mobile Computing ,July 2014