Indian J.Sci.Res. 17(2): 411-415, 2018

ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

IDENTIFYING PACKET DROPPING ATTACKS IN WAN

[1] K.Poorna Surya Teja, [2]K.Vigneswara Reddy, [3]B.Sanjeev , [4] Ms. G. Yamini
[1,2,3,4] Department of InformationTechnology,Sreenidhi Institute of Science &Technology, Hyderabad.

Abstract —Th Interest to determine the Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network. Here observing a cycle of packet losses in the network and losses are caused by link errors only, or by the combined effect of link errors and malicious drop. Inside-attack caused by malicious nodes as parts of the route utilize their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance. Because packet dropping rate in this case of similar 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 develop the correlations between lost packets.

Furthermore, to ensure a calculation of these correlations, here we develop a homomorphic linear authenticator (HLA) based public auditing architecture that allows to detector verify the reliability of the packet loss information reported by nodes. The construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To decrease the estimation of the baseline scheme of packet-block-based mechanism is allow proposing the one trade detection accuracy for lower computation complexity. Through wide-ranging simulations, verifying the proposed mechanisms accomplish the significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection

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. 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.

First, the continuous presence of extremely high packet loss rate at the malicious nodes makes this type of attack easy to be detected. Second, once being detected, these attacks are easy to mitigate. For example, in case the attack is detected but the malicious nodes are not identified, one can use the randomized multi-path routing algorithms to circumvent the black holes generated by the attack, probabilistically eliminating the attacker's threat. If the malicious nodes are also identified, their threats can be completely eliminated by simply deleting these nodes from the network's routing table. 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 amount 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, the authors have shown that an 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. 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

[1] **Corresponding Author**

channel conditions (e.g., fading, noise, and interference, a.k.a., 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. The above problem has not been well addressed in the literature. As discussed in Section 2, most of the related works preclude the ambiguity of the environment by assuming that malicious dropping is the only source of packet loss, so that there is no need to account for the impact of link errors.

On the other hand, for the small number of works that differentiate between link errors and malicious packet drops, their detection algorithms usually require the number of maliciously-dropped packets to be significantly higher than link errors, in order to achieve an acceptable detection accuracy. 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. 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. The basic idea behind this method is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the stochastic processes that characterize the two phenomena exhibit different correlation structures (equivalently, different patterns of packet losses).

Therefore, 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. Our algorithm takes into account the cross-statistics between lost packets to make a more informative decision, and thus is in sharp contrast to the conventional methods that rely only on the distribution of the number of lost packets. 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., reflect the actual status of each packet transmission. Such truthfulness is essential for correct calculation of the correlation between lost packets. This challenge is not trivial, because it is natural for an attacker to report false information to the detection algorithm to avoid being detected. For example, the malicious node may understate its packet-loss bitmap, i.e., some packets may have been dropped by the node but the node reports that these packets have been forwarded.

Therefore, some auditing mechanism is needed to verify the truthfulness of the reported information. 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. Our solution to the above public-auditing problem is constructed based on the homomorphic linear authenticator (HLA) cryptographic primitive, which is basically a signature scheme widely used in cloud computing and storage server systems to provide a proof of storagefrom the server to entrusting clients. However, direct application of HLA does not solve our problem well, mainly because in our problem setup, there can be more than one malicious node along the route. These nodes may collude (by exchanging information) during the attack and when being asked to submit their reports. For example, a packet and its associated HLA signature may be dropped at an upstream malicious node, so a downstream malicious node does not receive this packet and the HLA signature from the route. However, this downstream attacker can still open a back-channel to request this information from the upstream malicious node.

When being audited, the downstream malicious node can still provide valid proof for the reception of the packet. So packet dropping at the upstream malicious node is not detected. Such collusion is unique to our problem, because in the cloud computing/storage server scenario, a file is uniquely stored at a single server, so there are no other parties for the server to collude with. We show that our new HLA construction is collusion-proof. Our construction also provides the following new features. First, privacy-preserving: the public auditor should not be able to decern the content of a packet delivered on the route through the auditing information submitted by individual hops, no matter how many independent reports of the auditing information are submitted to the auditor. Second, our construction incurs low communication and storage overheads at intermediate nodes.

This makes our mechanism applicable to a wide range of wireless devices, including low-cost wireless sensors that have very limited bandwidth and memory capacities. This is also in sharp contrast to the typical storage-server scenario, where bandwidth/storage is not considered an issue. Last, to significantly reduce the computation overhead of the baseline constructions so that they can be used in computation-constrained mobile devices, a packet-block-based algorithm is proposed to achieves scalable signature generation and detection. This mechanism allows one to trade detection accuracy for lower computation complexity.

II.Existing System

The most of the related works preclude the ambiguity of the environment by assuming that malicious dropping is the only source of packet loss, so that there is no need to account for the impact of link errors. On the other hand, for the small number of works that differentiate between link errors and malicious packet drops, their detection algorithms usually require the number of maliciously-dropped packets to be significantly higher than link errors, in order to achieve an acceptable detection accuracy.

Depending on how much weight a detection algorithm gives to link errors relative to malicious packet drops, the related work can be classified into the following two categories.

The first category aims at high malicious dropping rates, where most (or all) lost packets are caused by malicious dropping.

The second category 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.

Disadvantages Of Existing System

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. This problem has not been well addressed in the existing system.In the existing system first category case, the impact of link errors is ignored.In the second Category, Certain knowledge of the wireless channel is necessary in this case.

III.Proposed System

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. 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.

The basic idea behind this method is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the stochastic processes that characterize the two phenomena exhibit different correlation structures (equivalently, different patterns of packet losses). Therefore, 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.

Our algorithm takes into account the cross-statistics between lost packets to make a more informative decision, and thus is in sharp contrast to the conventional methods that rely only on the distribution of the number of lost packets.

Advantages Of Proposed System

1. The proposed system with new HLA construction is collusion-proof.

2. The proposed system gives the advantage of privacy-preserving.

3. Our construction incurs low communication and storage overheads at intermediate nodes. This makes our mechanism applicable to a wide range of wireless devices, including low-cost wireless sensors that have very limited bandwidth and memory capacities. This is also in sharp contrast to the typical storage-server scenario, where bandwidth/storage is not considered an issue.

4. Last, to significantly reduce the computation overhead of the baseline constructions so that they can be used in computation-constrained mobile devices, a packet-block-based algorithm is proposed to achieves scalable signature generation and detection. This mechanism allows one to trade detection accuracy for lower computation complexity.

Ad Hoc Wireless Network Diagram
Internet
Broadband modem
Ethernet or USB cable
Computer 2
Wi-Fi
Computer 1
Printer
Wi-Fi
Computer 4
PDA
iPhone
Computer 3

Module Description

Service Provider:

In this module, the service provider browses the file and sends to the particular end users via router. And also service provider can assign energy and assign distances for the nodes in router.

Router:

In this module, the router sends the file from source to destination (from service provider to end users) by selecting shortest distances between two nodes & sufficient node energy. And if node has less energy than file size then packet dropper in router drops the some packets from file and sends remaining file to th destination. And it can also do some operations like
view distances, view energy, view files, viewattackers, verify, refresh.

Auditor:

In this module, the auditor discovers the traffic pattern,means it stores the details of dropped packets. I contains details of in which node packets are dropped,how many no of packets dropped, from which filedropped & status of packets.

Destination (End User):

In this module, there are n no of destinations (A, B,C….). These end users only receive the file from service provider via router. While getting the file from service provider there may be chances of packets dropping, if packets are dropped then end user will gets dropped packets from point to point manager. The end users receive the file by without changing the File Contents. Users may receive particular data files within the network only.

Attacker:

Attacker is one who makes changes the energy of particular nodes in router. And all attackers' details stored in router with their all details such as attacker Ip address, attacked node, modified energy and attacked time.

IV.Conclusion

In this paper, we showed that 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. We developed an HLA-based public auditing architecture 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. In addition, in this paper we have assumed that source and destination are truthful in following the established protocol because delivering packets end-to-end is in their interest. 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 secondorder 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 our future studies.

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 untrusted stores,‖ in Proc. ACM Conf.

[3.] Comput. and Commun. Secur., Oct. 2007, pp. 598–610. G. Ateniese, S. Kamara, and J. Katz, ―Proofs of storage from homomorphic identification 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] 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. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.

[6] 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.

[7] D. Boneh, B. Lynn, and H. Shacham, ―Short signatures from the weil pairing,‖ J. Cryptol., vol. 17, no. 4, pp. 297–319, Sep. 2004.

[8.] 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.

[9.] L. Buttyan and J. P. Hubaux, ―Stimulating cooperation in selforganizing mobile ad hoc networks,‖ ACM/Kluwer Mobile Netw. Appl., vol. 8, no. 5, pp. 579–592, Oct. 2003.

[10] .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.

[11]. J. Eriksson, M. Faloutsos, and S. Krishnamurthy, ―Routing amid colluding attackers,‖ in Proc. IEEE Int. Conf. Netw. Protocols, 2007, pp. 184–193.

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

[13.] 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 Proc. IEEE Int. Conf. Commun., 2009, pp. 1062–1067.

[14] .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.

[15] D. B. Johnson, D. A. Maltz, and J. Broch, ―DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks,‖ in Ad Hoc Networking. Reading, MA, USA: Addison-Wesley, 2001, ch. 5, pp. 139–172.