Detection of Packet Dropping Attacks for Privacy Preservation in Wireless Ad-Hoc Networks

Supriya[1] Arun Kumar H[2]
[1,2]Assistant Professor
[1]Rajiv Gandhi Institute of Technology, Mumbai, India
[2]Reva Institute of Technology and Management, Bangalore, India

Abstract— There are usually two types of packet dropping attacks observed in the network. Link error and malicious packet dropping are the sources for packet losses in multi-hop wireless ad hoc network. In this paper, while observing a number of packet losses in the network, one should concentrate on how the packets are lost in a network, whether the packets dropped are caused by link errors only or by the combinational effect of link errors and malicious dropping. Here, particularly certain cases are displayed where it's one of nodes in the network, whereby malicious nodes exploit their knowledge of the routing context to drop a small amount of packets that are critical to the network performance. Because the packet dropping rate in this case is similar to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. For the enhancement of the detection accuracy, a scheme to attain the interrelationships between lost packets is proposed. Furthermore, to ensure truthful calculation of these correlations, development of a Homomorphic Linear Authenticator (HLA) based public auditing architecture that allows the detector to validate the truthfulness of the packet drop information reported by nodes. This establishment is privacy preserving, collaboration proof, and incurs low communication and limited storage.

Key words: Homomorphism Linear Authenticator, Auto-Correlation Function, Attack Detection Request, Malicious Attack, Denial-of-Service, Packet-Block-Based Mechanism

I. INTRODUCTION

In a multi-hop wireless network, nodes cooperate in relaying/routing traffic. An opponent can exploit this cooperative nature to commence 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. Ultimately, such a severe Denial-of-Service (DoS) attack can paralyze the network by partitioning its topology.

Yet importunate packet dropping can effectively degrade the performance of the network, from the attacker's stance 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 effortless to be detected. Second, once being detected, these attacks are easy to diminish. A malicious node that is part of the route can exploit its acquaintance of the network protocol and the communication context to launch an insider attack–an attack that is sporadic, but can achieve the same performance deprivation effect as a persistent attack at a much lower risk of being detected. Specifically, the malicious node may estimate the importance of various packets, and then drop the small amount that are deemed highly vital to the operation of the network.

In this paper, a precise algorithm has been developed for detecting selective packet drops made by insider attackers. This algorithm also provides a truthful and publicly authentic 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 successive 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 portray the two phenomena exhibit different correlation structures (consistently, different patterns of packet losses). Therefore, by detecting the correlations between lost packets, one can decide whether the packet loss is solely due to regular link errors, or is a combined effect of link error and malicious drop. This algorithm takes into account the cross-statistics between lost packets to make a more informative decision, and thus is in sharp contrast to the predictable methods that rely only on the distribution of the number of lost packets.

II. RELATED WORK

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

The first category aims at elevated malicious dropping rates, where most (or all) lost packets are caused by malicious dropping. In this case, the influence of link errors is ignored. Most related work falls into this category. 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 malicious node that continues to drop packets will ultimately 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 neighbours to supervise and identify misbehaving nodes. A node with a high packet dropping rate is given a ghastly reputation by its neighbours. This reputation details is propagated cyclically throughout the network and is used as a key metric in selecting routes. Subsequently, a malicious node will be expelled 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. The fourth sub-category addresses the problem

using cryptographic methods. 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 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. The traffic at the MAC layer of the source node according to a certain statistical distribution, so that intermediate nodes are able to estimate the rate of received traffic by sampling the packet arrival times.

III. PROPOSED SYSTEM

Consider a multi-hop network which is having an arbitrary path as shown in figure. The source node sends the packets through intermediate nodes to the destination node. In each hop, the sending node is called as an upstream node of a receiving node. The packets are transmitted from source to destination and a bitmap is obtained for each node as (a1, a2….am) where aj=0 or 1. If the packet is successfully transmitted then aj=1 and if the packet is not transmitted the value of aj is considered as 0. By using this bitmap we can find the correlation between the lost packets. From this correlation we can find the malicious node.

There is an auditor in the network which is independent. The meaning of independent is that it is not related with any of the nodes in the network and it don't know about the secrets associated with the nodes. Here auditor is capable of detecting attacker's node when it gets request from the source. After sending all the packets from source to destination, the destination sends a feedback to source about the route i.e whether the route is under attack or not by considering some parameters. After getting feedback, if the route seems to be under attack then source will send the attack detection request (ADR) to auditor. Now auditor starts investigation to find malicious node. The auditor requests certain information from the intermediate nodes. Here normal nodes reply with correct information and the malicious node try to cheat. Here each and every node must reply for the auditor request otherwise the node is considered to be misbehaving.

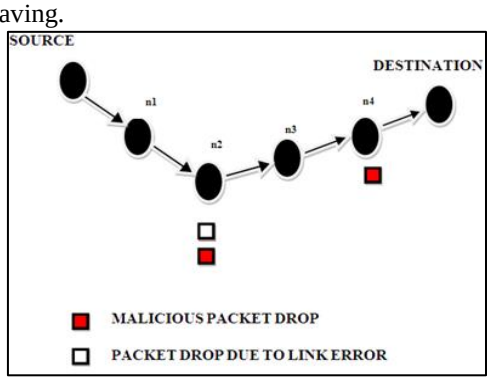

Fig. 1: Network Attack Model

The main challenge here is for the guaranty of the information sent by the nodes to the auditor. The attacker usually sends the wrong information not to get detected. Sometimes the malicious node may drop the packet and will send that that the packet is transmitted. To overcome this problem the usage of Homomorphic linear authenticator (HLA) a cryptographic method which is used in cloud computing and can truthfully detect the malicious node.

A. Advantages

High detection accuracy, Privacy Preserving: The public auditor should not be able to discern the content of a packet delivered on the route through auditing information submitted by individual hops.

B. Disadvantages

Due to signature generation overhead may be high.Data confidentiality will raise the issue in this work.

IV. CONCLUSION AND FUTURE WORK

In comparison 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 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 which allows one to trade detection accuracy for lower computation complexity.

Some open issues remain to be explored in the future work. Mechanisms are limited to static or quasi-static wireless ad hoc networks. Frequent changes on topology and link characteristics have not been considered along with extension to highly mobile environment. In addition, assumption 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 the future research.

The implementation and optimization under various particular protocols will be considered in the future studies.

REFERENCES

[1] Y. Zhang, L. Lazos, and W. Kozma. "AMD: audit-based misbehavior detection in wireless ad hoc networks." IEEE Transactions on Mobile Computing, to appear.

[2] 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.

[3] T. Shu, M. Krunz, and S. Liu. "Secure data collection in wireless sensor networks using randomized dispersive routes." IEEE Transactions on Mobile Computing, 9(7):941–954, 2010.

[4] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer. "Castor: Scalable secure routing for ad hoc networks." In INFOCOM, 2010 Proceedings IEEE, pages 1 –9, march 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] G. Ateniese, S. Kamara, and J. Katz. "Proofs of storage from homomorphic identification protocols." In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), 2009.
[7] 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.
[8] 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.
[9] W. Kozma Jr. and L. Lazos. "Dealing with liars: misbehavior identification via Renyi-Ulam games." In Proceedings of the International ICST Conference on Security and Privacy in Communication Networks (SecureComm), 2009.
[10] 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 TISSEC, 10(4), 2008.
[11] H. Shacham and B. Waters. Compact proofs of retrievability. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), Dec. 2008.
[12] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), pages 598–610, Oct. 2007.
[13] J. Eriksson, M. Faloutsos, and S. Krishnamurthy. Routing amid colluding attackers. 2007.
[14] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan. An acknowledgement-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5):536–550, May 2006.
[15] K. Balakrishnan, J. Deng, and P. K. Varshney. TWOACK: Preventing selfishness in mobile ad hoc networks. In Proceedings of the IEEE WCNC Conference, 2005.
[16] 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.
[17] Q. He, D. Wu, and P. Khosla. Sori: a secure and objective reputationbased incentive scheme for ad hoc networks. In Proceedings of the IEEE WCNC Conference, 2004.
[18] S. Zhong, J. Chen, and Y. R. Yang. Sprite: a simple cheat-proof, creditbased system for mobile ad-hoc networks. In Proceedings of the IEEE INFOCOM Conference, pages 1987–1997, 2003.
[19] R. Rao and G. Kesidis. Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited. In Proceedings of the IEEE GLOBECOM Conference, 2003.
[20] G. Noubir and G. Lin. Low-power DoS attacks in data wireless lans and countermeasures. ACM SIGMOBILE Mobile Computing and Communications Review, 7(3):29–30, July 2003.
[21] Y. Liu and Y. R. Yang. Reputation propagation and agreement in mobile ad-hoc networks. In Proceedings of the IEEE WCNC Conference, pages 1510–1515, 2003.
[22] S. Buchegger and J. Y. L. Boudec. Performance analysis of the confidant protocol (cooperation of nodes: fairness in dynamic ad-hoc networks). In Proceedings of the ACM MobiHoc Conference, 2002.
[23] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the ACM MobiCom Conference, pages 255–265, 2000.

