

# Privacy - Preserving and truthful detection of packet dropping attacks in wireless ad hoc networks

R.Saravanan<sup>1</sup>, S.Gopinath<sup>\*2</sup>

<sup>#</sup>Computer science and Engineering Department,  
gnanamani college of technolog, namakkal,  
Anna University – Chennai

**Abstract**-Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network. While observing a sequence of packet losses in the network, whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop are to be identified. 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. 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, the correlations between lost packets is identified. Homomorphism 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 construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead of the baseline scheme, a packet-block based mechanism is also proposed, which allows one to trade detection accuracy for lower computation complexity.

## 1. 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.

### 1.1 ADVANTAGES OF PRIVACY PRESERVING

#### High malicious dropping rates:

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.

#### Cryptographic Methods:

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.

#### 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 maliciously node

that continuous to drop packets will eventually deplete its credit, and will not be able to send its own traffic.

#### Reputation systems:

A reputation system 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.

#### 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.

## 2. RELATED WORK

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. 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.

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 maliciously node that continuous to drop packets will eventually 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 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.

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. Existing work utilizes Bloom filters 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 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.

### 3. PROPOSED SYSTEM

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., reflect 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 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 storage from the server to entrusting clients.

### 4. CONCLUSION AND FUTURE WORK

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 quasistatic 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 crypto-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 our future studies.

### REFERENCES

- [1] J. N. Arauz. 802.11 Markov channel modeling. Ph.D. Dissertation, School of Information Science, University of Pittsburgh, 2004.
- [2] 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.

- [3] 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.
- [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 TISSEC, 10(4), 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 Transactions on Information System Security, 10(4):11–35, 2008.
- [6] K. Balakrishnan, J. Deng, and P. K. Varshney. TWOACK: preventing selfishness in mobile ad hoc networks. In Proceedings of the IEEE WCNC Conference, 2005. [7] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. Journal of Cryptology, 17(4):297–319, Sept. 2004.
- [8] 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.
- [9] L. Buttyan and J. P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applications, 8(5):579–592, Oct. 2003.
- [10] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring. Modelling incentives for collaboration in mobile ad hoc networks. In Proceedings of WiOpt, 2003.