International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-5,May 2016
ISSN: 2395-3470
www.ijseas.com

PRIVACY PRESERVING POLICY TO DETECT THE PACKET AUDITED BY USING HLA IN WIRELESS SENSOR NETWORKS

K.Swathi[1], K.Nagalakshmi[2]

P.G Scholar[1], Assisitant Professor[2]

Department of Computer Science and Engineering[1, 2]

KLN College of Information Technology, Pottapalayam, TamilNadu [1, 2]

Abstract

Link error and malicious packet dropping are two foundations for packet losses in multi-hop wireless ad hoc network. When perceiving a sequence of packet losses in the network, whether the losses are caused by link errors, or by the combined effect of link errors and malicious drops are to be recognized. 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. Homomorphic linear authenticator (HLA) based public auditing architecture is established that permits 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.

Keywords- packet dropping; data gathering; H L A ; network traffic; wireless sensor networks

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 it was 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.

In [1] related work can be classified into the following two categories. It aims at high malicious dropping rates, where most (or all) lost packets are caused by malicious dropping. In this case, the influences of link errors are ignored. Most related work falls into this category. Based on the methodology is used to identify the attacking nodes, these works can be further classified into four sub-categories.

The first sub-category is based on the 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 from its neighbors. This reputation information is propagated periodically throughout the network and is used as an important metric in selecting routes. Subsequently, 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 build 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.

In [2][3] 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 respite of the paper is organized as follows. Section presents the related work and Section introduces the proposed scheme, and Section evaluates the performance of it by computer simulation. Finally, Section concludes the paper and outlines future research direction.

2. Related Works

2.1 The Existing Approaches

The related work can be classified into the following two categories.

In[1] 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.

In [2] 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 system [3] 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. In [4][5]End-to end or hop-to-hop acknowledgements **t**o directly locate the hops where packets are lost. A hop of high packet loss rate will be excluded from the route.

Cryptographic methods Bloom filters [6] 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 targets [7] 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.

Drawbacks

- Most of the related works assumes that malicious dropping is the only source of packet loss.
- For the credit-system-based method, a malicious node may still receive enough credits by forwarding most of the packets it receives from upstream nodes.
- In the reputation-based approach, the malicious node can maintain a reasonably good reputation by forwarding most of the packets to the next hop.
- While the Bloom-filter scheme is able to provide a packet forwarding proof, the correctness of the proof is probabilistic and it may contain errors.
- As for the acknowledgement-based method and all the mechanisms in the second category, merely counting the number of lost packets does not give a sufficient ground to detect the real culprit that is causing packet losses.

3.The Proposed Scheme

We first discuss the system model and energy model used in the proposed routing scheme.

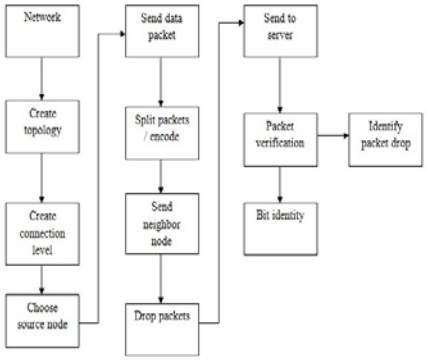

Fig1 System Architecture

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 elect 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 an individual node 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 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.

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 the auditing information submitted by individual hops
- Incurs low communication and storage overheads at intermediate nodes

3.1 System Model

The system model and energy model used in the proposed routing scheme are

- Network model
- Independent auditor
- Setup phase
- Packet drop detection
- Packet Status
- Node Block

3.2 Network model

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.

3.3 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}.

3.4 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 send through the route to destination. Destination after receiving packets can verify the packet and after verification it can decrypt the packets.

3.5 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.

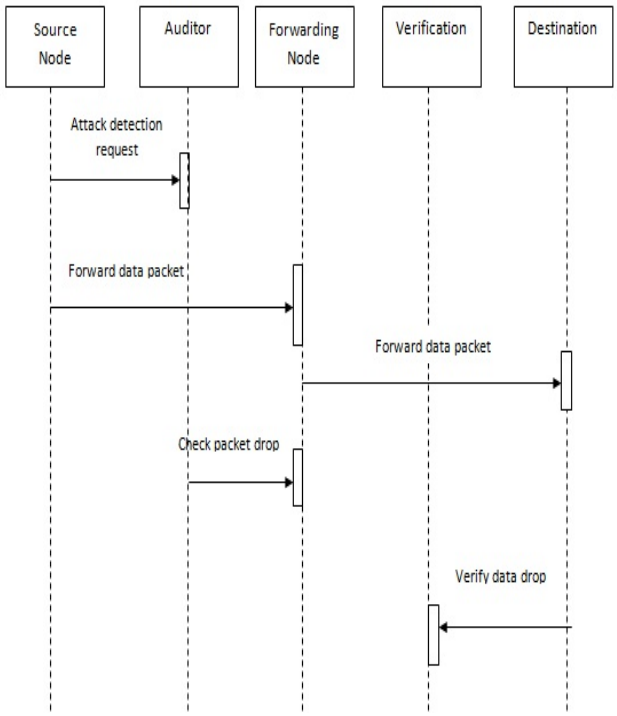

Fig 2 Sequence diagram

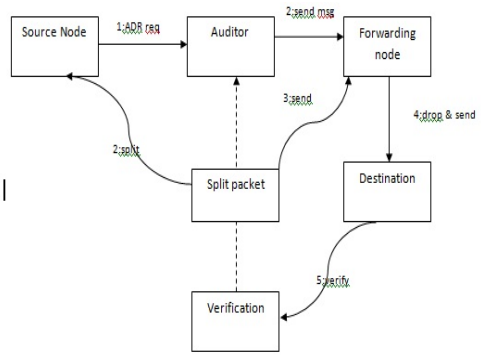

Fig 3 Collaboration Diagram

3.6 Packet Status

When packets are sending from the source to destination, it will pass through the middle ware nodes. So that the packet may leads to drop. After it reaches the destination, the status of the packet is generated by using the Homomorphic Linear Authenticator algorithm (HLA). HLA generates the Auditor, and the auditor is responsible for packet Status. By which we can know about the losses of packet.

3.7 Node Block

In this module, the auditor blocks the node, which leads to packet dropping. So that the dropped data is being surveyed by the auditor and it was passed to the destination through the help of another node.

4. 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 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 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 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.