International Journal of Research in Engineering, Science and Management
Volume-2, Issue-1, January-2019
www.ijresm.com | ISSN (Online): 2581-5792

Detection of Malicious Packet Dropping in Wireless Ad Hoc Networks

S. Anusha[1], R. Jaya[2]

[1]M. Tech. Student, Dept. of Computer Science and Engg., New Horizon College of Engg., Bangalore, India

[2]Sr. Assistant Professor, Dept. of Computer Science and Engg., New Horizon College of Engg., Bangalore, India

***Abstract*: Security has been a hot topic nowadays and it has become one of the major issues caused. It has attracted a lot of research and development in past few years. The packet loss in the network is caused either due to the link error or malicious packet dropping or by the combined effect of both. We will detect this by observing the sequence of pattern in the network. 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. The technique called Homomorphism linear authenticator (HLA) based public auditing architecture is developed that allows the detector to verify the truthfulness of the packet. This technique provides privacy preserving, collusion proof, and incurs low communication and storage overheads. The persistent packet dropping can effectively degrade the performance of the network from the attacker's point. First the continuous presence of the extremely high packet loss rate at the malicious node makes this type of attacks easy to be detected. Once the attack has been detected it is easy to remove the attacker. In the proposed work we will be re-routing the packet in presence of the attacker.**

***Keywords*: Auditing, AES, Homomorphism linear authentication, packet re-routing.**

1. Introduction

In a multi-hop wireless ad-hoc network, the nodes cooperate with each other for getting the routing information. Exchanging of their routing information helps us to send the sensitive data through the network. If an attacker is found in the network the attacker might exploit the network. This may cause the denial of services packet dropping or many modifications in the original content. Because all these kinds of attacks the receiver will not be receiving the packet which was sent by the sender. The attacker first behaves as a cooperative node in the network, once being included in the route he starts dropping the packets slowly. In most of the cases the malicious nodes just simply stop forwarding the packets to link node. Denial of service attack may change the network by partition it into the topology. A malicious node which may be part of the route may explore the knowledge of the network protocol and communication content to launch an attack. The persistent packet dropping an effectively degrade the performance of the network. First the continuous presence of the extremely high packet loss rate at the malicious node makes this type of attacks easy to be detected. Once the attack has been detected it is easy to remove the attacker. In the proposed work we will be re-routing the packet in presence of the attacker. We will be updating the trust value for each node and if the trust value of the node is less than certain threshold we will be terming that node as an attacker or a malicious packet dropper. If the node is safe then the trust value of the node will be increased and the packet will be forwarded to the sink node.

2. Literature survey

[1] *Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks*

Author: Tao Shu and Marwan Krunz, Fellow, IEEE

The packet losses in the network can be caused by link errors or by malicious packet dropping in a multi-hop wireless adobe network. By observing the pattern of packet losses in the network. We will be determining whether the packet dropper only or by the combined effect of link error and malicious packet drops. In this paper we will be using homomorphic linear authenticator to verify the truthfulness of the packet. In this packet block based mechanism is used. Through extensive simulation we verify that the proposed mechanism achieves better detection accuracy than conventional methods.

[2] *Routing amid colluding attackers*

Author: J. Eriksson, M. Faloutsos, and S. Krishnamurthy

In presence of the colluding attackers in a secure wireless routing, we have proposed a first practical solution to these attackers. We are using a very secure routing protocol called sprout. The sprout continuously tries new routes to the destination, so this makes sprout resilient to the attacker. In this paper the security analysis and simulation results have shown that sprout is able to quickly find working parts in networks of hundreds of nodes and attackers. Overall sprout consistently delivers high and reliable performance.

[3] *On maximizing collaboration in Wireless Mesh Networks without monetary incentive*

Author: Gabriel Popa; Eric Gourdin ; Franck Legendre ; Merkouris Karaliopoulos

In a distributed network the nodes are not under the control of the single administrative entity. The fulfillment of network operations is highly dependent on their cooperation. In this paper we focus on static wireless mesh networks and also we look into the issues of selfishness in the packet forwarding.

Firstly, we look at the dependencies merge in these network as a result of topologies. Traffic demand matrix our results shows that the cooperation increases when the flow increases. We use dependency model to drive the selection of routes in the network. The study investigates the resulting trade of amount network through put sever traffic flows and routing stretch factor.

[4] *Combining cryptographic primitives to prevent jamming attacks in wireless networks Author*

Author: Ngangbam Herojit Singh; A. Kayalvizhi

In a wireless medium it provides an intentional interference attack which is referred as jamming. Jamming is addressed under a external threat model. The adversaries with internal knowledge of the protocol and the network can launch low effort jamming attacks that are difficult to detect. In the proposed work we address the problem of jamming attack and attackers in short period of time. To mitigate these attacks, we develop three schemes that prevent real time packet classification by combining cryptographic primitives with physical-layer attributes. They are Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), All-Or-Nothing Transformation Hiding Schemes (AONTS-HS).

3. Problem statement

The packets can be dropped due to link error or by the malicious packet drop. The packet drop can also be caused by the combined effect of both the reasons. Detecting attackers in a highly dynamic wireless environment is extremely challenging. The challenging task comes when we need to not only detect the place where the packet is dropped but also identify whether the packet that was dropped was intentional or unintentional. Due to the open nature of wireless ad hoc medium, a packet dropping can be caused by harsh channel conditions e.g.; fading, noise and interference, link or by insider attacker. In this case just by observing the packet loss rate is not enough to accurately identify the exact cause of packet loss.

4. System modules

The system contains four modules.

- Network modeling.
- Independent auditing.
- Setup phase.
- Packet dropping detection
- Packet re-routing

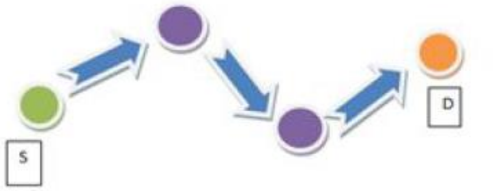

Fig. 1. Intermediate nodes with source and destination

A. *Networking modeling*

The wireless channel consists of nodes which are randomly placed in network. The wireless channel is consisting of each hop along PSD (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 are forwarded to the next node so that they reach the destination, and packets transmitted during the bad state are lost and are not reaching the destination. A sequence of M packets is transmitted consecutively over the channel.

B. *Independent auditing*

There is an independent auditor Ad in the network. Ad is independent which means it’s not depended on any node in PSD. The auditor is responsible for detecting malicious nodes on demand in the network so that they can be detected and packets will not be forwarded to that node. Specifically, it is assumed A receives feedback from B when B suspects that the route is under attack. Ad needs to collect certain information about the route in PSD so that the packet can be forwarded.

C. *Setup phase*

The setup phase takes place right after route PSD is established, but before any data packets are transmitted over the route. The setup phase will tell the route in which the packet can forwarded safely without the attacker or any packet dropping. The sender encrypts the message which it as to forward and the destination after receiving the message the message is decrypted and read.

D. *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.

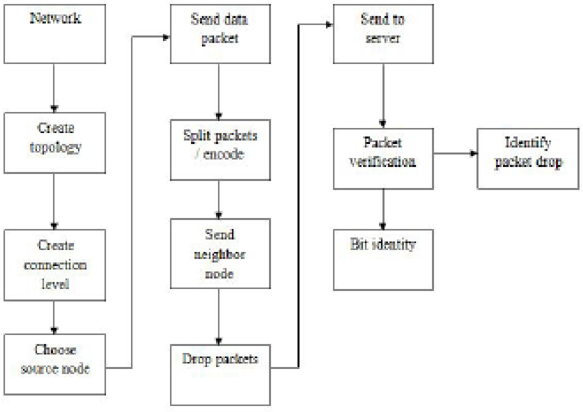

Fig. 2. System architecture

E. Packet re-routing

After the packet dropper has been identified we will be finding another routing path for transferring the packet to the sink node. We will be finding the trust value for each node based on this trust value will be allowing the node for transferring the packet. If the node is found as an attacker, we will be lowering the trust value less than certain threshold and if the node is safe then the trust value will be increased. We will continuously be finding the route and keep updating the trust value of the nodes and will be finding the best route for reaching the sink node.

5. Result

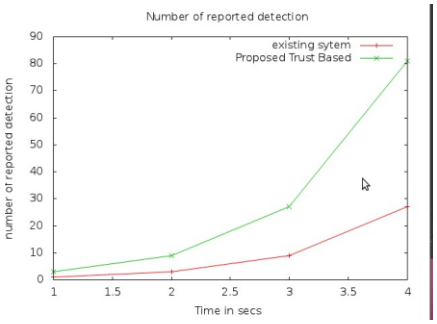

Fig. 3. The graph here shows how the performance as improved over the existing system. The number of attackers is detected better in the proposed system.

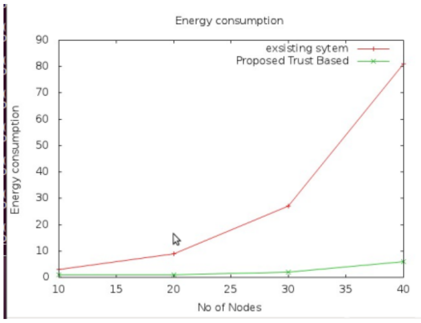

Fig. 4. This graph shows the energy consumption of the system. The proposed work consumes less energy compared to existing system.

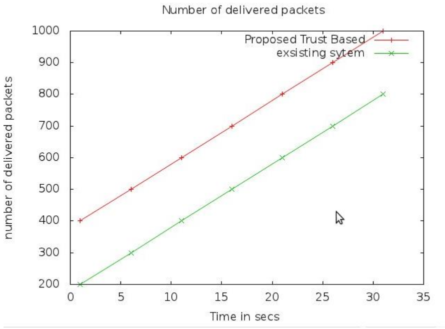

Fig. 5. The packet delivery of packets in the proposed is being improved compared to the existing work.

6. Conclusion

It is compared with conventional detection algorithms that uses 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. We have improvised the existing work by re-routing of the packets when the attackers are found. We will be updating the trust value for each node and based upon the trust value the packets are forwarded and the malicious packet droppers are identified. 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.

References

[1] T. Shu and M. Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks," in *IEEE Transactions on Mobile Computing*, vol. 14, no. 4, pp. 813-828, 1 April 2015.

[2] J. Eriksson, M. Faloutsos and S. V. Krishnamurthy, "Routing amid Colluding Attackers," *2007 IEEE International Conference on Network Protocols*, Beijing, 2007, pp. 184-193.

[3] N. H. Singh and A. Kayalvizhi, "Combining cryptographic primitives to prevent jamming attacks in wireless networks," *2013 International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, 2013, pp. 251-255.

[4] G. Popa, E. Gourdin, F. Legendre and M. Karaliopoulos, "On maximizing collaboration in Wireless Mesh Networks without monetary incentives," *8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, Avignon, 2010, pp. 402-411.