International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016 [ICSSCCET 2016]

ISBN	978-81-929866-6-1	**VOL**	02
Website	icssccet.org	**eMail**	icssccet@asdf.res.in
Received	25 – February – 2016	**Accepted**	10 - March – 2016
Article ID	ICSSCCET102	**eAID**	ICSSCCET.2016.102

Survey on Detection of Packet Dropping Attacks in Wireless Ad-Hoc Networks

R Geethpriya[1], L Kavitha[2], M Subhashini[3], G Shree Lekha Switha[4]
[1,2,3,4]Student Scholar, Department of Information Technology, Karpagam Institute of Technology, Coimbatore.

Abstract: *For the past few years, security has attracted many researchers and developers to concentrate more on it. The two sources of attacks in multi-hop wireless ad hoc networks for packet loss are link error and malicious packet dropping. The attack happens either by link error or malicious packet dropping or by combining effects of both link error and malicious drop, and this identified by observing a sequence of packet losses in the multi hop wireless ad hoc network. But in the case of insider-attack, malicious nodes that are part of the route use their knowledge of the communication context to selectively drop a small amount of packets that are critical to the multi hop network performance. The packet loss rate in existing algorithms are not satisfied because detection accuracy of packet dropping rate in this case is comparable to the channel error rate. To improve the detection accuracy, exploit the correlations between lost packets. To ensure truthful calculation of these correlations homomorphic linear authenticator (HLA) based public auditing architecture is used that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This results in privacy preserving, collusion proof, and incurs low communication and storage overheads. To decrease the computation overhead, a packet-block-based mechanism is also developed, which allows one to detect accuracy for lower computation complexity.*

I. INTRODUCTION

By collecting the mobile ad hoc nodes, we are creating the network infrastructure dynamically without using any existing network or centralized administration. Nodes cooperate in relaying/routing traffic in multi-hop wireless network. This adversary may make to launch several attacks. There were many security threats arise against mobile ad hoc networks, they are vulnerable and complicated of their preserve connectivity characteristics. A serious threat to mobile ad hoc networks said to be "Packet Drop Attack" is addressed. Credit system provides the solution for this problem. In this system, node receives credit by passing packets for others, and uses its credit to send its own packets. As a result, malicious node will start to drop packets and eventually loss the credit, and will not be able to send its own packet. Another solution is the reputation system that monitors and identifies the misbehaving nodes by its neighboring nodes. A bad reputation of a node is rated by the high packet dropping rate. This reputation information is used as an important metric in selecting routes throughout the networks. Bloom filter is another construct to enhance proofs for forwarding the packets at each node. We should examine the relayed packets at successive hops to identify suspicious hops that exhibit high packet loss rates.

II. Related Work

A.1.Credit-Based Systems

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. Proposed a system in which nodes receive credit for each packet they forward, and spend their accumulated

Cite this article as: R Geethpriya, L Kavitha, M Subhashini, G Shree Lekha Switha. "Survey on Detection of Packet Dropping Attacks in Wireless Ad-Hoc Networks". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 512-514. Print.

credit to transmit their own packets. This is accomplished through the use of a counter called the nuglet counter. The nuglet counter is incremented each time the node forwards a packet, and decremented each time the node transmits its own packet. The nuglet counter cannot take on a negative value and cannot be arbitrarily changed by the node.

B.2. Reputation Based System

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. A scheme which relies on two modules, the watchdog and the path rater. The watchdog module monitors the behavior of their next hop node by operating their radio in promiscuous mode. Once a node forwards a packet to the next hop, the node overhears to verify that the next hop node faithfully forwarded the packet. The scheme is based on the assumption that links between nodes are bi-directional and nodes utilize omni-directional antennas. A cache is used to store packets that wait for verification. If packets remain in the cache longer than a threshold period, the watchdog makes an accusation of misbehavior

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.

C.3. Route Discovery

When a source node wants to communicate with a destination, it must search the network until either the destination is found or another node has a route to the destination. Due to the lack of infrastructure, and/or possible mobility, ad hoc networks rely on on-demand routing protocols to discover routes.

Most on-demand routing protocols implement route discovery using a controlled network flooding mechanism. Examples include the Dynamic Source Routing (DSR) and the Ad hoc On-Demand Distance Vector (AODV) protocols. The route discovery module of AMD is based on such controlled-flooding techniques, but accounts for the reputation of individual nodes.

D.4. Acknowledgment-Based Systems

Acknowledgment-based systems verifies whether the messages received is forwarded to next hop. A scheme was proposed called as TWOACK, where nodes send 2-hop acknowledgment messages (TWOACK) to verify the transmission. When a node receives a packet, it sends a TWOACK along the reverse path, verifying that the intermediate node has faithfully forwarded packet. Packets which are not verified still remains in a cache until they get expire. A value (i.e. the total number of unverified packets) is assigned tots to determine the nodes that possess misbehaviour. Improved on TWOACK by proposing 2ACK. Similar to TWOACK, nodes explicitly send 2-hop acknowledgments (2ACK) to verify cooperation. To reduce overhead, 2ACK allows for only a percentage of packets received to be acknowledged. Additionally, 2ACK uses a one-way hash chain to allow nodes in the routing path to verify the origin of packets they are acknowledging, thus preventing attacks in which a misbehaving node drops the original packet and forwards a spoofed packet. Padmanabhan and Simon proposed a method called secure traceroute to identify the link on which misbehavior is occurring. Instead of the standard traceroute operation, which relies on nodes responding to expired packets, secure traceroute verifies the origin of responses and uses traceroute packets that are indistinguishable from data packets. Secure traceroute proceeds hop by hop, although instead of responding to expired packets, the source establishes a shared key with the node. By encrypting the packets, secure traceroute packets are indistinguishable from data packets and cannot be selectively dropped.

A Message Authentication Code (MAC) is utilized for authenticating the packets origin. Although traceroute is considered a reactive approach, secure traceroute is proactive, requiring connected nodes to transmit "keep-alive" packets when they have data to send. Xue and Nahrstedt [62] proposed the Best-effort Fault-Tolerant Routing (BFTR) scheme, which relies on end-to-end acknowledgment messages to monitor packet delivery ratio and select routing paths which avoid misbehaving nodes. Similar to the DSR routing protocol, the source floods RREQ messages to discover a routing path to a destination. However, RREP packets must be sent along the reverse path and must be signed with a shared secret key between the source and destination. Also, the destination responds to multiple RREQ, thus providing the source with multiple paths to choose from.

The source selects the shortest path for packet routing. During transmission to the destination, the source monitors the feasibility of the routing path, based on the end-to-end acknowledgments sent by the destination. Using a proposed heuristic, the source varies the routing path to maintain feasibility. Thus, the goal of BFTR is to avoid misbehaving nodes.

Cite this article as: R Geethpriya, L Kavitha, M Subhashini, G Shree Lekha Switha. "Survey on Detection of Packet Dropping Attacks in Wireless Ad-Hoc Networks". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 512-514. Print.

Conclusion

Detecting selective packet-dropping attacks in wireless ad hoc networks is extremely challenging in currently existing environment. The difficulty comes from the above method is that we need to not only detect the place (or hop) where the packet is dropped, but also identify whether the packet drop is intentional or unintentional .The conventional detection algorithms that utilize the distribution of the number of lost packets which exploits the correlation between lost packets and improves the accuracy in detecting the malicious packet drops. It is visible when the number of maliciously dropped packets is compared with those that are caused by link errors. In order to calculate the correct correlation between lost packets, it is critical to acquire truthful packet-loss information at individual nodes.

Reference

1. 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.
2. 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.
3. 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.
4. W. Kozma Jr. and L. Lazos, "Dealing with liars: Misbehavior identification via Renyi-Ulam games," presented at the Int. ICST Conf. Security Privacy in Commun. Networks, Athens, Greece, 2009.
5. K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgement- based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2006.
6. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom Conf., 2000, pp. 255–265.
7. V. N. Padmanabhan and D. R. Simon, "Secure trace route to detect faulty or malicious routing," in Proc. ACM SIGCOMM Conf., 2003, pp. 77–82.
8. A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," IEEE Trans. Depend. Secure Comput., vol. 9, no. 1, pp. 101–114, Jan./Feb. 2012.
9. R. Rao and G. Kesidis, "Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited," in Proc. IEEE GLOBECOM Conf., 2003, pp. 2957–2961.
10. Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," IEEE Trans. Mobile Comput., PrePrint, Vol. 99, published online on 6 Sept. 2013.

Cite this article as: R Geethpriya, L Kavitha, M Subhashini, G Shree Lekha Switha. "Survey on Detection of Packet Dropping Attacks in Wireless Ad-Hoc Networks". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 512-514. Print.