International Research Journal of Advanced Engineering and Science
ISSN: 2455-9024

Privacy-Preserving Detection of Packet Dropping Using Dynamic Link State Routing Distribution Algorithm

K. Thenmozhi[1], G. Sudhakar[2]
[1, 2]Computer Science & Engineering, Anna University, Chennai, Tamil Nadu, India-641109
Email address: [1]thenmozhircse46@gmail.com

Abstract*—Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network. 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, we propose to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, we develop a link state routing protocol (LSRP) based dynamic routing privacy preserving protocol architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This architecture is privacy preserving, collusion proof, and incurs low communication and storage overheads.*

***Keywords*—** *Packet droping, secure routing, attack detection, auditing.*

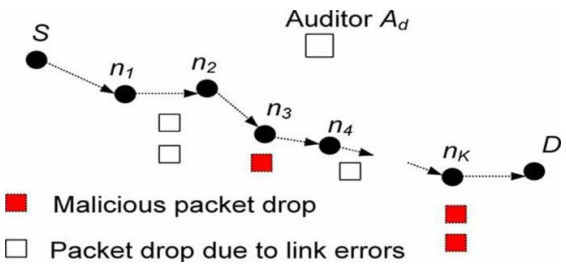
I. INTRODUCTION

Overview

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. First, the continuous presence of extremely high packet loss rate at the malicious nodes makes this type of attack easy to be detected. Second, once being detected, these attacks are easy to mitigate. For example, in case the attack is detected but the malicious nodes are not identified, one can use the randomized multi-path routing algorithms to circumvent the black holes generated by the attack, probabilistically eliminating the attacker's threat. If the malicious nodes are also identified, their threats can be completely eliminated by simply deleting these nodes from the network's routing table.

II. RELATED WORKS

Depending on how much weight a detection algorithm gives to link errors relative to malicious packet drops, 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. For example, the work in 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. Similarly, the method in traces the forwarding records of a particular packet at each inter- mediate node by formulating the tracing problem as a Renyi-Ulam game. The first hop where the packet is no longer forwarded is considered a suspect for misbehaving.



This is because the difference in the number of lost packets between the link-error-only case and the ink-error-plus-

K. Thenmozhi and G. Sudhakar, "Privacy-preserving detection of packet dropping using dynamic link state routing distribution algorithm," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 2, pp. 139-141, 2016.

malicious dropping case is small when the attacker drops only a few packets. Consequently, the detection accuracy of these algorithms deteriorates when malicious drops become highly selective. Our study targets the challenging situation where link errors and malicious dropping lead to comparable packet loss rates.

III. PROPOSED SYSTEM

The proposed architecture accepts the network parameters as input which contains the NS2 simulator where the dynamic routing privacy preserving algorithm is applied to the wireless ad hoc network. In a multi-hop wireless ad hoc network, packet losses are attributed to harsh channel conditions and intentional packet discard by malicious nodes. In this paper, while observing a sequence of packet losses, we are interested in determining whether losses are due to link errors only, or due to the combined effect of link errors and malicious drop. We are especially interested in insider's attacks, whereby a malicious node that is part of the route exploits its knowledge of the communication context to selectively drop a small number of packets that are critical to 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, we propose to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, we develop a link state routing protocol (LSRP) based dynamic routing privacy preserving protocol architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This architecture is privacy preserving, collusion proof, and incurs low communication and storage overheads. Through extensive simulations, we verify that the proposed mechanism achieves significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection. Malicious nodes can take advantage of this covert channel to hide their misbehavior and reduce the chance of being detected. For example, an upstream malicious node may drop a packet on Path of source to destination (PSD), but may secretly send this packet to a downstream malicious node via the covert channel. When being investigated, the downstream malicious node can provide a proof of the successful reception of the packet. This makes the auditor believe that the packet was successfully forwarded to the downstream nodes, and not know that the packet was actually dropped by an upstream attacker.

IV. WORKED MODULES

A. Link State Routing Protocols

Link state Routing path selection based on the shortest path is usually energy saving optimized. So different metrics are considered and weight is assigned to each link. Between two end-to-end nodes, there usually exists more than one route. In the potential relay node set, there will be relatively energy optimal routes that can achieve the least cost based on the nodes' battery capacity and propagation loss of the links. The research work have a simple multi-hop Hetro-network, with the relay node set R between the source and destination, and the immediate neighbor set R^* for each node. There exists an energy efficient route, for example, the route with relay nodes A, B, and C. Links with less propagation power loss and nodes with higher residual battery capacity are preferred. So the problem is simplified to minimize the power consumed during transmission and maximize the battery capacity of the next node to be used that is to minimize:(p(i))/((g(i)) i∈ R^* (1) for local (the immediate next hop) optimization Σ_(i∈R)▒(p(i))/(g(i)) i∈R (2) for global (all end-to-end hops) optimization where g(i) is the residual battery capacity of the ith node, and p(i) is the power cost per packet from node i-1 to node I (that it, Joules per second per packet). A detailed study of the Lithium-Ion battery discharging property is presented. The voltage decrease and the battery capacity are non-linear functions of discharging time: the lower the capacity remains, the faster the battery voltage drops. The residual battery capacity can be evaluated as the amount of energy remains in the battery, that is, the time duration for the battery to discharge when the transmitter is consuming power. The residual battery capacity is reduced for the amount of energy consumed by the transmitter. If we define f(i) = 1/g(i) and expand p(i), then (1) for local optimization will be (p(i))/(g(i))=[P_loss (i-1,i)+P_rx (i)+P_c (i)]·f(i) (3)where the power cost per packet p(i) from node i-1 to node i can be expanded to the sum of the power loss of this link (from node i-1 to i), the power cost to receive the packet at the ith node , and the power cost for routing messages to maintain this connection. The algorithm favors a link with less power loss and hence reduce the amount of energy consumed by potential re-transmission and link error. Usually the minimum threshold of receiving power of the receiver is constant (for instance, -80 dBm for current IEEE 802.11b cards) for all receivers (i.e, independent of the node index i). So the minimum value of prx(i) can be set as a constant prx. Since the routing messages for route discovery and maintenance are the same for all nodes for on-demand routing protocols, we can consider pc(i) a constant value pc too. Hence, both control and data packets are considered to consume energy according to their packet sizes. Note also that, when more link error occurs, more routing maintenance is needed and more energy is consumed.

Σ_(i∈R)▒(p(i))/(g(i))=Σ_(i∈R)▒〖f(i).〗 [P_loss (i-1,i)+P_rx (i)+P_c (i)].f(i (4) This algorithm can either optimize locally for each hop or globally for the end-to-end route between a source-destination For the global optimization, the data source will get to know the summation of the cost for all possible routes and decide which route to choose, based on the global cost function. While for local optimization, each intermediate node will choose locally a different next hop to forward data for energy efficiency from the local cost function. Global optimization tends to prefer routes with fewer hops (because cost function is a summation and is an implicit function of hop count) and hence can achieve less delay.

K. Thenmozhi and G. Sudhakar, "Privacy-preserving detection of packet dropping using dynamic link state routing distribution algorithm," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 2, pp. 139-141, 2016.

B. Dynamic Routing Privacy Preserving Routing Protocol

The dynamic routing selects routes based on the current state information for the network. The state information can be predicted or measured but the route will change depending on the available state information at the time of the traffic request. The privacy network can cope now with the dynamics of traffic and react to real-time network traffic accordingly, by introducing real-time behavior and state dependency in order to avoid congestion and to achieve optimal performance. Dynamic routing protocol is distinguished by two factors 1.The computational model that the routing service is using 2.The state information nature. There are two computational models used in dynamic routing the centralized and the distributive. The basic operation of privacy preserving is to allow a source to specify a destination area and simultaneously discover multiple nodes in it. However, to keep the description simple, we assume that only one node exists within each destination area. An alternate path through two links, A and B, with PP parameters (Privacy Preserving parameter on a link if that link is to be used as an alternative path) rA and rB, is considered least-loaded if it has the lowest value loadA, B where this quantity is often referred to as the PP permissibility of a path since it is a reflection of the bandwidth available in addition to the reservation parameters. A negative PP permissibility would indicate that an alternate route is not available while a large PP permissibility indicates an underutilized path. This is a computationally intensive routing logical decision to find the best route when any available route can carry the call but it's shown to have better performance than either Dynamic Non-Hierarchical Routing or homogenous routing protocol. The Dynamic routing protocol algorithm may prove extensible to multiple classes of service the network is currently operating in this mode.

C. Algorithm for Dynamic routing Protocol

Step 1 If the Source node S wants to send data to the destination node D, it will first send REQ message to all its neighbor.
Step 2 When neighbour nodes receive REQ message they will check their broadcast, if this packet's ID is already in their Cache then packet will be discarded.
Step 3 Otherwise, node will calculate its energy by using: Enew = Etx - Er + Eth + Em + Eover and send this value as a reply to source node.
Step 4 Source node will calculate the mean value of all the values of Enew of all the nodes and send a RREQ message to the node whose Enew value is nearest to the mean value.
Step 5 Assign the Attacker node depending on the routing environment.
Step 6 When the node receives a RREQ message it will send privacy preserving message to its own neighbours and this process will be continued till the destination node reaches.
Step 7 When destination node will receive the RREQ message it will send the RREP message back with the same route.

V. CONCLUSION

The goal of this proposed method is state that each transactions has been 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 Auditing Report. To correctly calculate the correlation between lost packets, it is critical to acquire truthful packet-loss information at individual nodes. We developed an link state routing protocol (LSRP) based dynamic routing privacy preserving protocol auditing architecture 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.

REFERENCES

[1] J. N. Arauz, "802.11 Markov channel modeling," Ph.D. Dissertation, School of Information Sciences, University of Pittsburgh, Pittsburgh, PA, USA, 2005.
[2] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 598-609, 2007.
[3] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," *Proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, pp. 319–333, 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 Transactions on Information and System Security (TISSEC)*, vol. 10, no. 4, pp. 1–35, 2008.
[5] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," *IEEE Wireless Communications and Networking Conference*, vol. 4, pp. 2137–2142, 2005.
[6] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.
[7] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," *Proceedings of the 3rd ACM International Symposium on Mobile ad hoc Networking & Computing*, pp. 226–236, 2002.

K. Thenmozhi and G. Sudhakar, "Privacy-preserving detection of packet dropping using dynamic link state routing distribution algorithm," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 2, pp. 139-141, 2016.