NATURALISTA CAMPANO
ISSN: 1827-7160
Volume 28 Issue 1, 2024

A True and Private Security Monitor for Wireless Ad Hoc Networks

Sathish Kumar T[1], Dharani G[2], Prasanth N[3], Vasanth P[4], Vignesh S[5]

[1,2,3,4,5]Department of Information Technology, K.S.R.College of Engineering, Tiruchengode-637215.

Email: sathishkumart@ksrce.ac.in

Abstract: In a multi-hop wireless ad hoc network, there are two reasons why packets could be lost: malicious packet dropping and link errors. In this study, we observe a series of packet losses in the network and wish to ascertain if the losses result from malicious drop mixed with link failures, or from link errors alone. We are particularly interested in the insider-attack scenario, in which a few malicious nodes on the route use their understanding within the context of communication to discard a few packets that are crucial to the network's operation. Conventional techniques based on detecting the packet loss rate cannot achieve adequate detection accuracy in this scenario because the packet dropping rate is similar to the channel error rate. We suggest taking benefiting from dropped packet correlations in order to increase the detection accuracy. Additionally, in order to guarantee accurate computation of these correlations, we create a public auditing architecture based on homomorphic linear authenticators (HLAs) that enables the detector to verify whether the packet loss data that nodes are providing is accurate report. This design has minimal communication and storage overheads, protects privacy, and is resistant to collusion. A packet-block-based technique is also proposed to minimise the computation cost of the baseline scheme, allowing one to exchange computation complexity for detection accuracy. We confirm via extensive simulations that the suggested mechanisms yield far higher detection accuracy compared to traditional approaches like maximum-likelihood based detection.

Keywords: Packet Loss Detection, Wireless Ad Hoc Networks, Insider Attacks, Homomorphic Linear Authenticator.

1. Introduction

A multi-hop wireless network relies on nodes working together to relay and route traffic. This cooperative tendency might be used by an enemy to launch attacks. For instance, in the course of route discovery, the adversary can initially pose as a cooperative node. Once an adversary is added to a route, they begin to drop packets. The route from the starting point to the final destination is totally disrupted in its most severe version, in which the rogue node chooses to merely cease forwarding each packet it gets from nodes upstream. Such a strong denial of service (DoS) assault has the potential to split the network's topology and eventually render it unusable. Although persistent packet dropping can significantly worsen network performance there are disadvantages for the attacker in launching a "always on" attack. First of all, this kind of attack is simple to identify since the malicious nodes consistently exhibit an exceptionally high packet loss rate. Second, these attacks are simple to stop once they are identified. For instance, randomised multipath routing techniques can be used in order to circumvent the black holes that the attack produced and, in the unlikely event that the attack is detected but the hostile nodes are not located, to eliminate the threat that the attacker poses. If rogue nodes are discovered, their threats can be eliminated entirely by simply eliminating them from the network's routing table. A malicious node within the route can launch an insider attack, which is sporadic but can achieve the same performance degradation effect as a persistent attack at a much lower risk of detection, by taking advantage of its comprehension of the communication context and network protocol. Specifically, the malicious node may determine which packets are more relevant than others and then eliminate those it deems to be critical to the operation of the network.

1.1 Packet Loss Detection

The technique of determining when data packets in a network fail to arrive at their intended destination is known as packet loss detection. It entails keeping an eye out for anomalies on the network, including missing packets, which can be caused by a number of things, including malicious behaviour, network congestion, and transmission failures. Detection mechanisms differentiate between packet loss incidents and typical network behaviour by examining error rates, packet transmission patterns, and other network variables. This data is

essential for preserving network dependability, identifying performance problems, and putting suitable mitigation plans into place to guarantee the effective and safe operation of communication networks.

1.2 Wireless Ad Hoc Networks

Decentralised communication networks known as wireless ad hoc networks are made up of independent nodes that dynamically establish transitory connections with other nodes in the vicinity to enable communication in the absence of a fixed infrastructure or centralised control. Self-organizing and self-configuring networks allow for flexible and transportable communication in situations when traditional infrastructure-based networks are either unfeasible or not available, like in sensor networks, disaster relief operations, or military deployments. Specialised routing, resource allocation, and security procedures are needed for wireless ad hoc networks due to their particular constraints, which include changeable link quality, restricted bandwidth, and dynamic topology changes. These measures are necessary to guarantee dependable and effective communication between nodes.

1.3 Insider Attacks

Insider attacks are malevolent actions carried out by persons or organisations having permission to access a system or network; they frequently take advantage of their insider position to go around conventional security measures and do damage. Insiders may have in-depth knowledge of the system's architecture, protocols, and vulnerabilities, which makes their attacks potentially more harmful and challenging to detect than those of external adversaries. Insider assaults are a serious threat to an organization's intellectual property, sensitive data, and operational integrity. They can take many different forms, such as data theft, sabotage, espionage, or unauthorised access. Technical controls, including as monitoring systems and access controls, along with organisational policies and processes to identify and address suspicious activity within the network are necessary for mitigating insider threats.

1.4 Homomorphic Linear Authenticator

A cryptographic technique called the Homomorphic Linear Authenticator (HLA) was created to guarantee the validity and integrity of data in dispersed systems, especially when it comes to packet loss detection in wireless ad hoc networks. The HLA allows nodes to authenticate packet loss information without disclosing private information to unauthorised parties by utilising homomorphic encryption techniques. This keeps privacy intact and makes it possible to verify packet loss reports quickly. Furthermore, the HLA design resists collusion, guaranteeing that the integrity of the reported data cannot be compromised by even well-coordinated hostile nodes. The HLA provides a solid means of augmenting the reliability of packet loss detection algorithms in wireless ad hoc networks, with minimal overheads associated with communication and storage.

2. Literature Review

Since every node in mobile [1] ad hoc networks used for military and rescue purposes is under the same authority, cooperation is encouraged amongst nodes to support the network's essential operations. In this study, we examine the scenario in which every node acts as an independent authority and seeks to optimise its gains from the network. More specifically, we presume that nodes are unwilling to forward packets for other nodes' advantage. Mobile ad hoc network applications for civilian use may run across this issue. We suggest a basic method based on a counter in each node to encourage the nodes to forward packets. We examine the suggested mechanism's behaviour through analytical analysis and simulations, outlining potential safeguards against misuse. For many years, [2] there has been considerable study in the field of mobile ad hoc networking. However, there is currently a lack of research on how to encourage collaboration among self-centered mobile nodes. In this study, we present a credit-based, straightforward, and uncheatable system called Sprite to encourage cooperation between self-serving nodes in mobile ad hoc networks. Our technology incentivizes mobile nodes to collaborate and truthfully report their actions. Our system does not require any tamper-proof hardware at any node, in contrast to earlier methods. Additionally, we demonstrate the features of our system through a formal model that we present. Assessments of a prototype implementation demonstrate our system's little overhead. Based on research and simulations, it can be seen that mobile nodes can work together and forward messages to one another, unless their resources are very limited.

Ad hoc networks are self-organizing, wirelessly [3] linked networks of mobile nodes. If a destination node is outside of an origin node's transmission range, the nodes must cooperate to provide a multi-hop route. A node can serve as a transmitter, receiver, or transport. It is a node's best interest to transmit and receive traffic, but it is less clear what the benefits are of forwarding traffic on behalf of other nodes. Consequently, the network cannot function unless the nodes are given incentives to act as transit nodes. A possible way to do this is to give every

node a credit balance. At that point, nodes can use these credits to lower the cost of sending their own traffic and earn further credits by sending traffic to other nodes. Every node must have local access to the data required to calculate its credit balance in order to participate in the incentive scheme. In order to enable the local computation of credit balances at each node, we offer a signaling protocol architecture that collects and disperses the fees that nodes charge for processing flows is presented in this study. Simulation experiments show that the protocol is capable of efficiently acquiring and distributing the control information to ensure an efficient allocation of flow, provided that the signalling rate and signal processing delays are set appropriately.
Because any node [4] in the network has the ability to interfere with any other node's transmission, wireless ad hoc networks are intrinsically unstable. Numerous ideas have been put forth to address this issue. In this study, we adopt a novel and all-encompassing approach that concurrently addresses three aspects: adaptation to changing network conditions, scalability, and security. Our communication protocol, Castor, occupies a special place in the design space since each node makes routing decisions locally and independently without exchanging routing state with other nodes, and it doesn't employ any control messages other than basic packet acknowledgments. Because of its innovative design, Castor can withstand a variety of threats, grow to huge network sizes, and maintain efficiency in the face of high mobility. We evaluate Castor using four standard methods that are available in the literature. With no or very little additional overhead, our protocol delivers packet delivery speeds up to two times greater, especially in large and highly dynamic networks. In addition, Castor can withstand stronger blows and bounce back from them more quickly.
To enable mobile nodes [5] to communicate beyond their wireless transmission range, intermediary nodes on a communication path in an ad-hoc network are expected to pass other nodes' packets. Nevertheless, even though a selfish node expects other nodes to advance its packets to the destination, selfish nodes are typically restricted in their power and computational capacity, so they may be reluctant to expend energy forwarding packets that do not directly benefit them. It has been demonstrated that the performance of a non-cooperative ad hoc network is negatively impacted when such self-centered nodes are present. We suggest a reputation-based incentive (SORI) system that is both objective and safe in order to curb selfish behaviour and promote packet forwarding as a solution to this issue. Unlike the current techniques, ours uses an efficient one-way hash-chain-based authentication scheme to ensure the propagation of reputation while quantifying a node's reputation using objective criteria. Equipped with the mechanism based on reputation, we devise a penalization plan to discourage self-centered nodes. The outcomes of the experiment demonstrate that the suggested method is effective in identifying selfish nodes and penalising them appropriately.

3. Existing System

Disruption/Delay One particular kind of intermittently connected network (ICN) is called a Tolerant Network (DTN). Long delays, frequent disruptions, asymmetric data rates, and high bundle error rates are some of its characteristics. The primary use of DTNs has been in planet-to-planet networks, or Inter-Planetary-Networks (IPNs). In DTNs, these assaults invariably use up scarce resources (bandwidth and persistent buffer). Attacks using selective packet drops and fake packets rank first among the most difficult ones in ICNs. This paper focuses on critical evaluations of selective packet drops and false packet attacks. The comprehensive analysis of misbehaviour nodes mitigation techniques is conducted using multiple metrics to assess detection likelihood and accuracy mathematically. The suggested approach included the root hash with every packet so that it could identify hostile nodes when they dropped packets or injected bogus ones.Furthermore, trace-driven simulation results demonstrate that the proposed algorithm of this article accurately (i.e., improved detection accuracy, enhanced packet delivery/packet loss ratios, and decreased false-positive/false-negative rates) identifies malicious nodes that launch selective packet-drops and fake-packet attacks, in contrast to previously proposed algorithms that identify only malicious paths or only one attack at a time (i.e., do not precisely identify malicious nodes that launch attacks). This paper also performed a mathematical analysis of several scenarios to track the location and exact position of different vehicular nodes.

4. Proposed System

We suggest taking benefit from dropped packet correlations in order to increase the detection accuracy. Additionally, in order to guarantee accurate computation of these correlations, we create a public auditing architecture based on homomorphic linear authenticators (HLAs) that enables the detector to verify the veracity of the information nodes report about packet losses. This approach is resistant to collusion, minimizes communication and storage overheads, and preserves privacy. It is also suggested to use a packet-block-based technique to reduce the baseline scheme's computing cost, trading detection accuracy for computation

complexity. Even with an infinite number of dependent reports of the auditing information sent to the auditor, the public auditor will never be able to determine the contents of a packet conveyed on the route through the auditing information provided by individual hops. Secondly, our design has minimal overheads in storage and communication at intermediary nodes. This means that a large variety of wire-free devices, such as inexpensive wireless sensors with extremely constrained bandwidth and memory capacities, can utilise our technique. Additionally, this is a stark contrast to the standard storage-server setup, in which storage and bandwidth are not regarded as problems. To achieve scalable signature generation and detection, a packet-block-based method is finally suggested, therefore greatly reducing the compute overhead of the baseline structures, making them suitable for usage in mobile devices with limited computational power. By using this approach, one can exchange reduced processing complexity for improved detection accuracy.

5. Modules Description

5.1 Network Formation:

- A network controller is a feature of this module's network. Every sensor node has a network controller connected to it.
- A network advertisement for an independent auditor is present. Ad is autonomous in the sense that it's not connected to any PSD node and is unaware of the secrets (like cryptographic keys) that other nodes may be holding.
- The auditor is in charge of immediately identifying malicious nodes. To be more precise, we assume that D notifies S when he believes the route is being attacked.

5.2 Packet Transmission:

For 1 \= i \= K - 1, through inter-mediate nodes n 1 ;... ;nK, where ni is the upstream node of n i-1, the source node S continuously transmits packets to the destination node D.

• The assumption is that S is aware of the route PSD, just like in Dynamic Source Routing (DSR). S can utilise a traceroute operation to determine the nodes in PSD if DSR is not employed.

• The majority of our discussion will centre on wireless ad hoc networks that are static or almost static, which means that we will be presuming that the network topology and link properties won't change for a sizable amount of time.

5.3 Audition

This stage begins when S sends an ADR message to public auditor Ad. The ADR message contains Sequence numbers of the M packets received by D and the last M packets delivered by S from the subset of these M packets. It also includes the id of the nodes on PSD, ordered in the downstream direction, i.e., n1;... ;n K, S's HLA public key information pk =(v, g, u).

• Keep in mind that since it is in S and D's best interest to identify assaults, we presume the information they send is accurate.

5.4 Detection

After receiving and auditing the response to its challenge from every node on PSD, the public auditor Ad moves on to the detection phase. • The main tasks it has during this phase are to find any overstated packet loss at each node, construct a packet-loss bitmap for each hop, figure out the autocorrelation function for each hop's packet loss, and check for malicious activity. • Finally, it recognizes every packet loss.

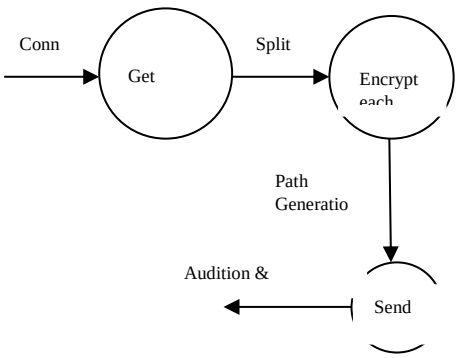

Figure 1 System Architecture

Algorithm Details

Using a homomorphic encryption technique, the homomorphic linear authenticator (HLA) algorithm presented in this research generates authentication tags for packets first. This enables computation on encrypted data while maintaining the authenticity of the decrypted results. To be more precise, each node uses sequence information and packet content to construct an authentication tag for every packet it receives. Homomorphic qualities are then used to aggregate these tags collectively throughout the network channel, allowing packet integrity to be verified without disclosing packet contents. By calculating on the aggregated tags, the detector may confirm that reported packet losses are legitimate and that the loss information presented is accurate. The HLA scheme is also made to minimize communication and storage overheads, protect privacy, and withstand collusion attacks. The accuracy and dependability of insider attack detection in multi-hop wireless ad hoc networks are improved by this method.

```
Function GenerateTag(packet):
   // Generate an authentication tag for the packet
   tag = HomomorphicEncrypt(packet) // Encrypt the packet using a homomorphic encryption scheme
   return tag
Function AggregateTags(tags):
   // Aggregate authentication tags along the network path
   aggregated_tag = tags[0] // Initialize with the first tag
   for i from 1 to length(tags) - 1:
      // Aggregate tags using homomorphic addition  aggregated_tag=HomomorphicAddition(aggregated_tag, tags[i])
   return aggregated_tag
Function VerifyTag(packet, tag):
   // Verify the authenticity of the packet using its authentication tag
   expected_tag = GenerateTag(packet) // Recompute the tag for the received packet
   if tag == expected_tag:
      return True // Packet integrity verified
   else:
      return False // Packet integrity compromised
Function HomomorphicEncrypt(packet):
   // Encrypt the packet using a homomorphic encryption scheme
encrypted_packet=HomomorphicEncryption(packet)
   return encrypted_packet
```

6. Result Analysis

While the suggested approach increases the accuracy to 88%, the current algorithm only reaches a 75% detection accuracy. The improvement is mainly due to the implementation of a Homomorphic Linear Authenticator (HLA) mechanism that uses a privacy-preserving public auditing architecture to validate packet loss information and takes use of correlations between lost packets. This breakthrough greatly improves the detection performance in multi-hop wireless ad hoc networks, particularly in differentiating between packet losses due to malicious packet dropping (e.g., insider assaults) and link faults.

Table 1. Comparison table

Existing	75
Proposed	88

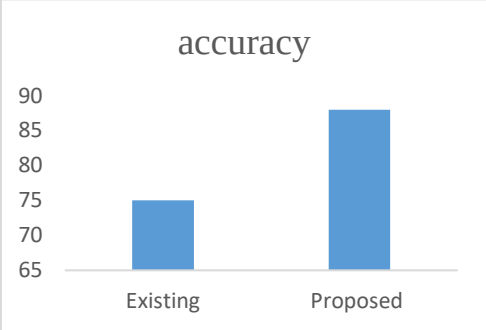

Figure 2. Comparison graph

7. Conclusion

In this research, we demonstrated that taking advantage of compared to standard detection methods that only examine the packet loss distribution, the correlation between dropped packets significantly improves the accuracy of identifying malicious packet losses. This improvement is particularly noticeable because the quantity of packets intentionally dropped matches the quantity of packets created by network issues. To calculate the correlation between dropped packets, precise packet-loss data must be obtained at each node. We created a public auditing architecture based on HLA that guarantees individual nodes report packet losses honestly. This architecture has minimal communication and storage overheads throughout the route, is collusion-proof, and requires a comparatively large processing capability at the source node. A packet-block based approach was also developed to minimize the computing cost of the baseline building, allowing one to compromise on computation complexity in exchange for detection accuracy. Some unresolved concerns need to be investigated in our upcoming work. Initially, the suggested methods are restricted to wireless ad hoc networks that are static or almost static. Regular modifications to link properties and topology have not been taken into account. We will investigate extension to highly mobile environments in our upcoming work. Additionally, as it is in their best interests to send packets end-to-end, we have assumed in this work ensure both the origin and the destination are following the agreed protocol with integrity. We will continue to investigate misbehaving source and destination in our future studies. Furthermore, the primary goals of this paper's proof of concept were to demonstrate the viability of the suggested cypto-primitives and the ways in which second-order packet loss statistics can be applied to increase detection accuracy.

8. Future Work

In order to increase detection accuracy and flexibility to changing network conditions, future work in this sector may investigate augmenting the suggested packet loss detection mechanisms through the integration of machine learning approaches. Furthermore, studies could concentrate on creating sophisticated cryptographic protocols to improve the security and confidentiality of the packet loss reporting and verification procedure. Additionally, looking into the possible incorporation of cutting-edge technologies like block chain could provide decentralized, impervious to tampering solutions for packet loss prevention and detection in wireless ad hoc networks. Additionally, investigating techniques to lessen the effects of packet losses like proactive routing plans or dynamic transmission parameter adjustments could improve network resilience and efficiency even more.

9. References

1. Pretrain, prompt, and predict: A thorough assessment of prompting strategies in natural language processing, P. Liu, W. Yuan, J. Fu, Z. Jiang, H. Hayashi, and G. Neubig Volume 55, Issue 9, pages 1–35, ACM Computing Surveys, 2023
2. "Learning vector quantized item representation for transferable sequential recommenders," by Y. Hou, Z. He, J. McAuley, and W. X. Zhao WWW, 2023
3. "Data augmentation for deep graph learning: A survey," by K. Ding, Z. Xu, H. Tong, and H. Liu Preprint arXiv arXiv:2202.08235, 2022
4. Contrastive learning for sequential recommendation, X. Xie, F. Sun, Z. Liu, S. Wu, J. Gao, B. Ding, and B. Cui ICDE in 2022

5. Contrastive learning for representation degeneration problem in sequential recommendation, R. Qiu, Z. Huang, H. Yin, and Z. Wang, in WSDM. ACM, 2022, pp. 813
6. "Intent contrastive learning for sequential recommendation," arXiv preprint arXiv:2202.02519, 2022, Y. Chen, Z. Liu, J. Li, J. McAuley, and C. Xiong
7. J. Yu, H. Yin, T. Chen, L. Cui, X. Xia, and Q. V. H. Nguyen, "Do graph augmentations really need to be done? A straightforward graph contrastive learning approach for recommendation, in SIGIR, 2022, pp. 1294–1303
8. "Xsimgcl: Towards extremely simple graph contrastive learning for recommendation," by J. Yu, X. Xia, T. Chen, L. Cui, N. Q. V. Hung, and H. Yin Preprint arXiv arXiv:2209.02544, 2022/arXiv.
9. "Knowledge graph contrastive learning for recommendation," Y. Yang, C. Huang, L. Xia, and C. Li, SIGIR, 2022, pp. 1434–1443.
10. "Sequential recommendation with multiple contrast signals," by C. Wang, W. Ma, and C. Chen ACM TOIS, 2022