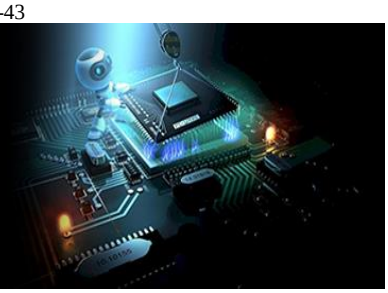
International Journal of Engineering in Computer Science



E-ISSN: 2663-3590
P-ISSN: 2663-3582
IJECS 2020; 2(2): 39-43
Received: 05-10-2020
Accepted: 09-11-2020

Paramjit
Research Scholar, Department of Computer Science and Engg, OSGU, Hisar, Haryana, India

Saurabh Charya
Dean and Associate Professor, Department of Computer Science and Engg, OSGU, Hisar, Haryana, India

Corresponding Author:
Paramjit
Research Scholar, Department of Computer Science and Engg, OSGU, Hisar, Haryana, India

Comparative analysis of proactive and reactive routing techniques in simulating black hole attacks

Paramjit and Saurabh Charya

DOI: https://doi.org/10.33545/26633582.2020.v2.i2a.103

Abstract
In wireless ad hoc networks, security is a critical concern due to their dynamic and distributed nature. One of the most challenging security threats in these networks is the black hole attack, where malicious nodes drop packets rather than forwarding them, leading to disruption in communication. To mitigate such attacks, various routing techniques have been proposed, including proactive and reactive approaches. This paper aims to provide a comprehensive analysis of proactive and reactive routing techniques in simulating black hole assaults. We delve into the characteristics, advantages, and limitations of each approach, providing insights into their effectiveness in combating black hole attacks.

In addition, it uses Roadside Units (RSUs) to communicate data and promote network-wide use. The performance of PAODV_RTPSN is evaluated thoroughly with the use of several important metrics, including the Packet Drop Rate (PDR), Average End-to-End Delay (E2ED), Jitter, Network Throughput (Th), and Network Routing Load (NRL). The study involves simulations with 500 nodes over 1000 seconds in NS2, comparing AODV, AODV under black hole attacks, and the proposed hybrid approach. The results demonstrate that PAODV_RTPSN significantly mitigates the adverse effects of black hole attacks, improving PDR, Th, E2ED, Jitter, and NRL. In conclusion, this research contributes a robust solution to the security challenge of black hole attacks in VANETs while upholding user anonymity. PAODV_RTPSN substantially improves network performance, making VANETs more resilient and trustworthy for drivers and authorities.

Keywords: VANETs, black hole attacks, hybrid approach, network security

Introduction

Wireless ad hoc networks have emerged as a crucial paradigm for communication in dynamic and decentralized environments where the infrastructure is either unavailable or impractical to deploy. These networks, characterized by their self-organizing nature and absence of fixed infrastructure, offer flexible connectivity among mobile nodes, making them ideal for scenarios such as disaster recovery, military operations, and sensor networks. However, the inherent openness and distributed nature of ad hoc networks also render them susceptible to various security threats.

Among the myriad of security challenges, black hole attacks stand out as particularly insidious. In a black hole attack, a malicious node within the network deliberately drops incoming packets without forwarding them to their intended destinations. This nefarious behavior disrupts communication and can severely impact the functionality and reliability of the network. Black hole attacks exploit the trust-based nature of routing protocols, exploiting vulnerabilities in route establishment and maintenance mechanisms.

Given the critical role of routing in facilitating communication within ad hoc networks, devising effective countermeasures against black hole attacks is imperative. Two prominent categories of routing techniques have emerged for this purpose: proactive and reactive. Proactive routing protocols establish and maintain routes proactively, anticipating communication needs in advance. In contrast, reactive routing protocols initiate route discovery only when needed, minimizing overhead but potentially leaving the network vulnerable to attacks.

This paper aims to delve into the proactive and reactive routing techniques employed to simulate and mitigate black hole assaults in wireless ad hoc networks.

By exploring the characteristics, vulnerabilities, and countermeasures associated with each approach, this study seeks to provide insights into their effectiveness in safeguarding against black hole attacks. Through comparative analysis and simulation-based evaluations, this research aims to shed light on the strengths and limitations of proactive and reactive routing techniques, guiding network designers and security practitioners in making informed decisions to enhance the resilience of ad hoc networks against malicious threats.

Literature Review

VANETs have recently been getting much attention because of the radical changes they could bring to the transportation industry. However, the widespread use of VANETs poses serious security concerns, such as exposure to black hole attacks and the necessity of protecting user anonymity. This literature overview of VANET security, black hole attacks, and anonymity studies provides context for our proposed hybrid strategy and focus on the state of the field.

VANET Security

Due to the potentially disastrous effects of a breach in VANET security, protecting these networks is paramount. Several different types of safety procedures have been advocated in academic writing. Messages sent through VANETs are typically encrypted and digitally signed to prevent unauthorised parties from reading them. However, there are restrictions on the usefulness and applicability of these methods, mainly when applied to the ever-changing context of vehicular networks [3] study emphasises the importance of developing more effective cryptographic solutions that can keep up with the fast-paced nature of VANETs. Security in VANETs is complicated by the fact that they are constantly evolving. It has been emphasised by [4] that these networks require robust security methods to protect the privacy, authenticity, and accessibility of information passing across them. The frequent topological shifts and disjointed connectivity of VANETs present substantial challenges for the use of conventional security mechanisms. Security measures must be flexible and practical to keep up with the ever-changing threat.

The environment in which VANETs function is highly dynamic, with vehicles constantly moving and the network's topology frequently shifting. For security measures, these communication limitations pose significant issues [5]. Maintaining a safe and efficient transportation system requires constant and dependable communication. Traditional security mechanisms, which frequently rely on stable and predictable network conditions, might be challenging to employ in a dynamic network environment like todays. Therefore, security solutions should be adapted to meet the specific communication constraints of VANETs while maintaining low latency. Multiple attack routes that potentially compromise the safety of VANETs have been uncovered using secondary sources [6]. These include manipulating messages, eavesdropping conversations, assuming another person's identity, and inserting malicious messages. Attackers can use these entry points to compromise the security of transportation networks and the safety of passengers and drivers. Protecting the confidentiality, integrity, and validity of transmitted data is crucial in VANETs since they rely on confidence between cars and infrastructure nodes. VANETs are vulnerable to these attack vectors due to their dynamic and open character, necessitating robust security methods to ward off danger [7].

Black Hole Attacks

Attacks from black holes are one of the most significant threats to VANETs. By making a misleading claim to be the "Shortest Path" between two specified sites, an adversary can prevent communications from reaching the receivers for whom they were intended. Several studies [8] have investigated the many strategies that can be used to identify and evade black hole attacks. Many of the currently available approaches suffer from high rates of false-positive and false-negative detection, which lowers their dependability in conditions that more closely resemble the actual world.

Anonymity Preservation

Maintaining the anonymity of users is another critical component of the security of VANETs. Users expect that their anonymity will be preserved during conversations in vehicles. In order to address this problem, several pseudonymous authentication systems [9] have been created. Vehicles can use these protocols to have confidential talks without leaving any trace in the digital world. Despite this, the research highlights that practical anonymity while maintaining security is a challenging goal to achieve. The fact that some pseudonymous systems are vulnerable to attacks that could lead to their de-anonymisation [10] is one factor that highlights the importance of exercising moderation.

Challenges and Limitations

Several difficulties and restrictions of existing VANET security solutions are shown in the literature. As highlighted by [11], standard cryptographic solutions need help keeping up with the ever-changing and extremely mobile nature of automotive networks. Real-time communication is essential for VANETs, and these systems may struggle to keep up.

Second, current methods for spotting and stopping black hole attacks frequently generate false positives and cannot spot more complex attacks. [12] Research highlighted the need for improved intrusion detection systems with higher accuracy and reliability. Third, even while pseudonymous authentication techniques protect users' privacy, they may be susceptible to attacks based on traffic analysis. In this shortcoming, [13] emphasised the need for additional study into ways to enhance the privacy-preserving properties of VANETs.

Our proposed hybrid strategy draws on and is guided by several previous studies [14]. Highlight using trust-based systems as a promising strategy. Black hole attack detection can benefit from trust models that use the actions of nearby cars to evaluate each one's reliability and spot outliers. While there is much literature on VANET security, there are still open questions that we hope to answer. A major shortcoming is the lack of a unified, effective method to address black hole attacks and privacy concerns. Existing research frequently prioritises one component at the price of another, preventing them from providing a comprehensive answer. In addition, VANETs' inherent volatility and the increasing complexity of threats call for creating more resilient and adaptable security systems. Our study proposes a novel hybrid VANET security and anonymity approach

combining cryptographic approaches, trust-based models, and pseudonymous authentication. The literature analysis has shown a pressing need to improve VANET security and anonymity, that current solutions have limitations, and that a more all-encompassing strategy is required. We suggest a hybrid strategy to address these shortcomings and furnish a more secure and confidential communication setting for vehicle networks.

Methodology

The proposed method is the PAODV_RTPSN Hybrid approach for blackhole attack prevention in VANET. This method's two-tiered security mechanism helps lower the overall network load, which is an issue even when only the most fundamental preventative measures are taken. At the end of the first level of security, the source node will switch to level 2 security if it detects a malicious node attempting to impose a black hole attack on the network. Level 2 security is based on establishing and next a trusted path mode for transmission. If the source node detects a hostile node, the node will switch to level 2 security. It will communicate information to other nodes using RSUs so all nodes can proceed along the Trusted Path together.

Algorithm

Step 1: the source node, which does not yet know where the target node is located, sends out a Route Request Message (RREQ). SN RREQ [SN_ID, DN_ID, SN_SEQ_NO, BROD_ID].

Step 2: Receiving Nodes process the RREQ broadcast by the Source Node and respond with a Route Reply Message (RREP) to the Sending Node. DN RREP [DN_ID, SN_ID, DN_SEQ_NO, HOP_COUNT, LIFE_TIME]

Step 3: Each node will initially save the Node Ids of its neighbours in a list called list trusted node.

Step 4: That node will be considered malicious if the source node receives a route reply from a node with a much more significant Sequence Number than the source's Sequence Number.

Step 5: switching to the trusted path mode, in a coordinated black hole attack, this is a huge boon. Once an entry in the trusted path is present, the source node will only send data through that path. In addition, each node will provide the appropriate RSU with a list of untrusted nodes.

Step 6: The RSU will compile a list of all non-trusted nodes from each node within the range and use that information to create a list of nodes to block. Each node in the RSU range will be sent this list of blocked nodes. To further facilitate trusted path-based transmission, RSU should also notify other nodes.

Analysis of PAODV_RTPSN IN VANET: Some of these factors were taken into account as performance metrics in this study; for example, the PDR, Network Throughput, and Average E2ED. We ran a 1000-second NS2 simulation with 500 virtual nodes. We will use the AODV procedure to conduct an analysis of the parameters in light of the discussion in section 4. To ensure an accurate outcome, we ran the simulation five times for each approach, and the data is shown in the tables below. First, we ran the AODV protocol simulation and obtained the result in Table 1. We then used a black hole attack, and the outcome was as shown in Table 2. We can pinpoint the decline in several metrics. After that, we put the simulation through its paces using the hybrid approach PAODV_RTPSN, and the outcome was as shown in Table3. The average results for each parameter across all methods are shown in Table 4.

Table 1: AODV Protocol Result

	PDR (%)	The (kbps)	E2ED (ms)	Jitter (ms)	NRL (%)
Observation1	3.93	552.70	84.17	0.0445	6.1761
Observation2	3.87	541.65	88.36	0.0454	6.1722
Observation3	3.82	550.49	87.04	0.0446	6.1690
Observation4	3.94	551.77	83.57	0.0445	6.1767
Observation5	3.96	545.84	89.11	0.0450	6.1780

Table 2: AODV Protocol under black hole Attack Result

	PDR (%)	Th (kbps)	E2ED (ms)	Jitter (ms)	NRL (%)
Observation1	88.64	64.56	467.06	0.1847	5.1220
Observation2	89.62	59.71	483.01	0.1998	5.1235
Observation3	88.92	63.41	468.43	0.1882	5.1295
Observation4	87.67	69.46	427.12	0.1717	5.1268
Observation5	88.66	65.14	438.92	0.1832	5.1231

Table 3: PAODV RTPSN Protocol under black hole Attack Result

	PDR (%)	Th (kbps)	E2ED (ms)	Jitter (ms)	NRL (%)
Observation1	15.22	486.9750	90.2340	0.0988	6.7049
Observation2	15.38	486.8287	90.1521	0.0989	6.7312
Observation3	14.85	487.3632	93.6890	0.0988	6.7084
Observation4	14.87	487.3633	93.6222	0.0995	6.7054
Observation5	15.08	486.8288	90.1521	0.0989	6.7314

Table 4: Different Protocol Result

	PDR (%)	Th (kbps)	E2ED (ms)	Jitter (ms)	NRL (%)
AODV	3.90	548.49	86.45	0.0448	6.1744
AODV Under Blackhole Attack	88.69	64.45	456.91	0.1855	5.1250
PAODV_RTPSN	15.08	484.71	93.02	0.0992	6.7110

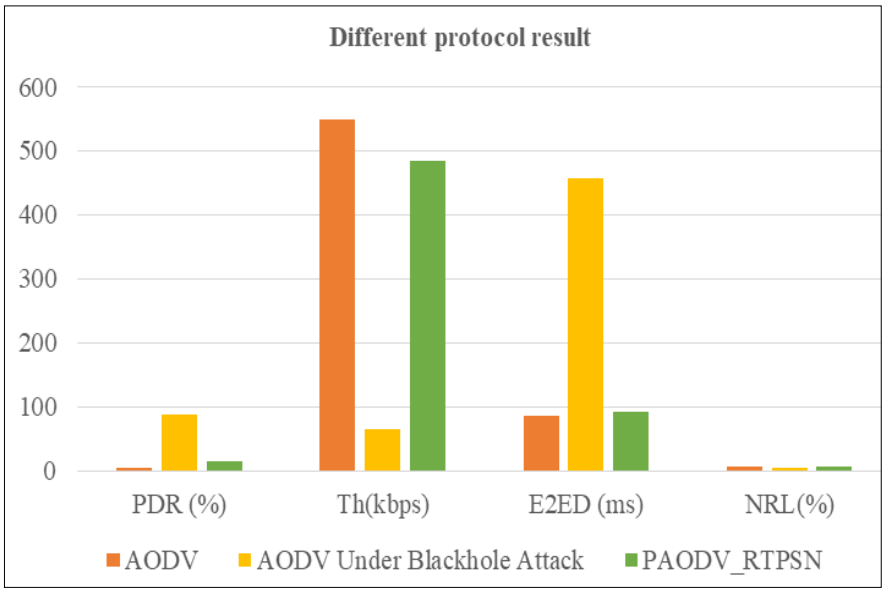


Fig 1: Different protocol result

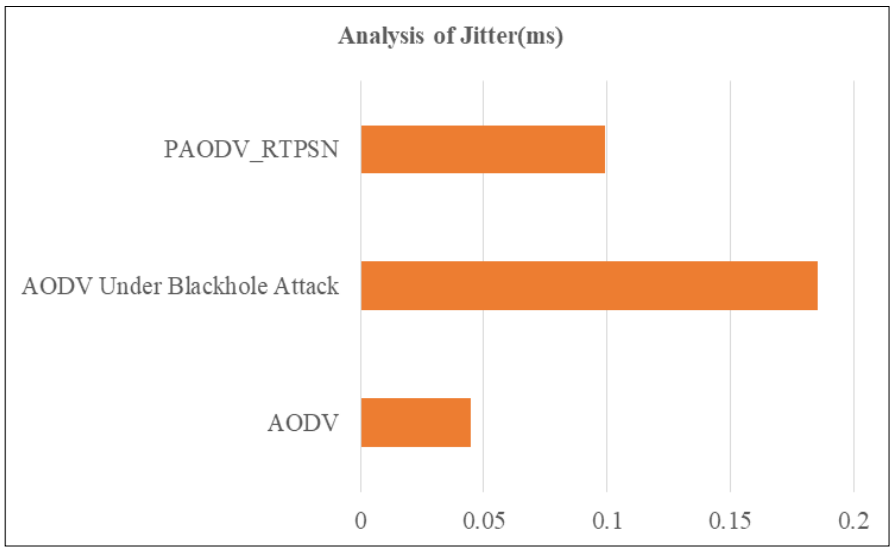


Fig 2: Analysis of Jitter

Analysis of packet loss, throughput, average E2ED, NRL (Figure 1) and jitter (Figure 2) for the AODV protocol, the AODV protocol that was subjected to a black hole attack, and the preventative AODV protocol with a reactive trusted path that was based on sequence number. Following a Blackhole Routing Attack, the average packet drop rate in AODV increased to 8.70 per cent from 3.90 per cent. This was a significant increase. We noticed tremendous progress after implementing the hybrid PAODV_RTPSN technique, as the percentage of lost packets decreased to 15.08%. Following a Blackhole Routing Attack, our throughput in AODV decreased to 64.46 kbps from a previous value of 548.49 kbps. After putting the hybrid PAODV_RTPSN method in place, we saw a boost in throughput that brought it up to 484.70 kbps. Before a Blackhole Routing Attack, the AETD for AODV was 86.45 milliseconds; however, it increased to 456.92 milliseconds after the attack. After implementing the hybrid strategy known as PAODV_RTPSN, the end-to-end delay that we measured on average was 93.03 milliseconds. Our AODV's Average Jitter was 0.0448 milliseconds before a Blackhole Routing Attack. However, it jumped to 0.1856 milliseconds after the attack. When we utilised the Hybrid technique PAODV_RTPSN, we discovered that the Average Jitter was 0.0993 milliseconds. Following a Blackhole Routing Attack, the results showed that the AODV technique had an average network routing burden of 6.1744%, while the PAODV_RTPS hybrid method had an average network routing load of 6.7110%. According to the findings, the hybrid strategy is superior to the conventional methods in every respect that was evaluated.

Conclusions

In this study, we addressed how blackhole attacks can harm VANETs and how the hybrid preventative technique AODV_RTPSN can help lessen the severity of the damage caused by this kind of routing assault. We analysed the effects of several factors and displayed the results using graphical representations. It is not enough to simply detect the rogue node to keep the network safe from further assaults; this step is necessary. Following implementing our hybrid method to blackhole routing attack protection, all aspects of the network, including the drop rate of packets, throughput, average E2ED, jitter, and Network Routing Load, saw considerable improvements.

References

1. Patcha A, Mishra A. Collaborative security architecture for black hole attack prevention in mobile ad hoc networks. In: Radio and Wireless Conference; c2003. RAWCON '03. Proceedings. DOI: 10.1109/rawcon.2003.1227896.
2. Malik M, Khan MZ, Faisal M, Khan F, Seo JT. An efficient dynamic solution for the detection and prevention of black hole attack in VANETs. Sensors. 2022;22(5):1897. DOI:10.3390/s22051897.
3. Primiero G, Martorana A, Tagliabue J. Simulation of a trust and reputation based mitigation protocol for a black hole style attack on VANETs. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS & PW); c2018. DOI: 10.1109/eurospw.2018.00025.
4. Mitra S, Jana B, Poray J. A novel scheme to detect and remove black hole attack in cognitive radio vehicular ad hoc networks (CR-VANETs). In: 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE); c2016. DOI: 10.1109/iccece.2016.8009589.
5. Grimaldo J, Marti R. Performance comparison of routing protocols in VANETs under black hole attack in Panama City. In International Conference on Electronics, Communications and Computers (CONIELECOMP); c2018. DOI: 10.1109/conielecomp.2018.8327187.
6. Jin H, Papadimitratos P. Scaling VANET security through cooperative message verification. In: 2015 IEEE Vehicular Networking Conference (VNC); c2015. DOI:10.1109/vnc.2015.7385588.
7. Kaur, Kaur J. Trust-based security protocol to mitigate black hole attacks in Mobile Adhoc Networks. DOI: 10.21203/rs.3.rs-2197795/v1.
8. Hravani PP, RR, HDS, VS, Nayak MM. Enhanced performance and security for MANETs against Blackhole attack Blackhole attacks. In: NCICCNDA. DOI: 10.21467/proceedings.1.14.
9. Fatiha M, Hafid H. Towards the development of vehicular ad-hoc networks (VANETs). In: IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks. DOI: 10.4018/978-1-7998-2570-8.ch002.
10. Younas S, *et al*. Collaborative detection of Black Hole and gray hole attacks for secure data communication in VANETs. Applied Sciences. 2022;12(23):12448. DOI: 10.3390/app122312448.
11. Weng JH, Chi PW. Multi-level privacy preserving K-anonymity. In: 2021 16th Asia Joint Conference on Information Security (Asia JCIS); c2021. DOI:10.1109/asiajcis53848.2021.00019.
12. Choi H, Nam Y, Shin Y, Lee E. The partial cloud member replacement for reconstructing vehicular clouds in VANETs: Reactive and proactive schemes. Ad Hoc Networks. 2022;136:102959. DOI: 10.1016/j.adhoc.2022.102959.
13. Xu H, Zeng M, Hu W, Wang J. Authentication-based vehicle-to-vehicle secure communication for VANETs. Mobile Information Systems. 2019;2019:1-9. DOI: 10.1155/2019/7016460.
14. Mirchev MJ, Mirtchev ST. System for DDOS attack mitigation by discovering the attack vectors through statistical traffic analysis. International Journal of Information and Computer Security. 2020;13(3/4):309. DOI: 10.1504/ijics.2020.10029285.