SECURING VANETs FROM GREY-HOLE ATTACKS USING TRUST-BASED MALICIOUS NODE DETECTION TECHNIQUES

Er. Sumanpreet Kaur,

Assistant Professor, College of Engineering & Management, Neighbourhood Campus Rampura Phul,

Punjabi University, Patiala

ABSTRACT:

Vehicular Ad-Hoc Networks (VANETs) are a critical component of intelligent transportation systems, enabling real-time communication among vehicles and infrastructure to ensure road safety and traffic efficiency. However, the dynamic and decentralized nature of VANETs makes them vulnerable to various security threats, particularly grey-hole attacks. In such attacks, malicious nodes selectively drop packets, disrupting communication and compromising network reliability. This research proposes a trust-based malicious node detection framework aimed at mitigating grey-hole attacks in VANET environments. The proposed technique evaluates the trustworthiness of nodes based on parameters such as packet forwarding behavior, communication consistency, and historical performance. Nodes exhibiting suspicious behavior are dynamically isolated from the network to maintain the integrity of data transmission. Simulation results demonstrate that the trust-based model significantly improves packet delivery ratio, reduces end-to-end delay, and enhances overall network resilience against grey-hole threats. This approach offers a lightweight, scalable, and effective solution for securing VANETs in real-time communication scenarios.

Keywords: VANETs (Vehicular Ad-Hoc Networks), Grey-Hole Attacks, Trust-Based Detection, Malicious Node Identification, Network Security, Packet Dropping, Node Trust Evaluation, Vehicular Communication, Intrusion Detection, and Secure Routing Protocols

1.Introduction:

The rapid advancement of wireless communication technologies has revolutionized modern transportation systems, leading to the emergence of **Vehicular Ad-Hoc Networks (VANETs)**. As a subclass of Mobile Ad-Hoc Networks (MANETs), VANETs play a pivotal role in enabling real-time communication among vehicles (vehicle-to-vehicle or V2V) and between vehicles and infrastructure (vehicle-to-infrastructure or V2I)[9]. This communication framework is integral to Intelligent Transportation Systems (ITS), facilitating road safety, traffic efficiency, accident avoidance, and infotainment services [10]. VANETs support applications such as collision warnings, traffic condition alerts, lane change notifications, and emergency vehicle routing—all of which demand high reliability, low latency, and robust security [11].

However, the **highly dynamic topology, decentralized architecture, and lack of centralized control** in VANETs expose them to various security threats [12]. One of the most insidious among these is the **grey-hole attack**. Unlike black-hole attacks where a malicious node drops all data packets it receives, a grey-hole attack involves **selective packet dropping**, making it more difficult to detect and more damaging over time. In such attacks, a node may behave normally during initial transmissions and later begin to drop specific packets, thus undermining trust and causing significant degradation in the **Quality of Service (QoS)** of the network [13].

Grey-hole attacks can lead to **route disruptions, data loss, network congestion, and reduced packet delivery ratio**, especially in safety-critical VANET applications[14]. Given the potential consequences of these attacks, it becomes imperative to develop efficient and intelligent mechanisms to identify and eliminate malicious nodes[15]. Conventional cryptographic solutions may not be feasible due to the real-time constraints and the computational overhead they impose on vehicular networks. Therefore, **lightweight, adaptive, and behavior-based security mechanisms are gaining prominence** in the field of VANET security[16] in show Figure.1.

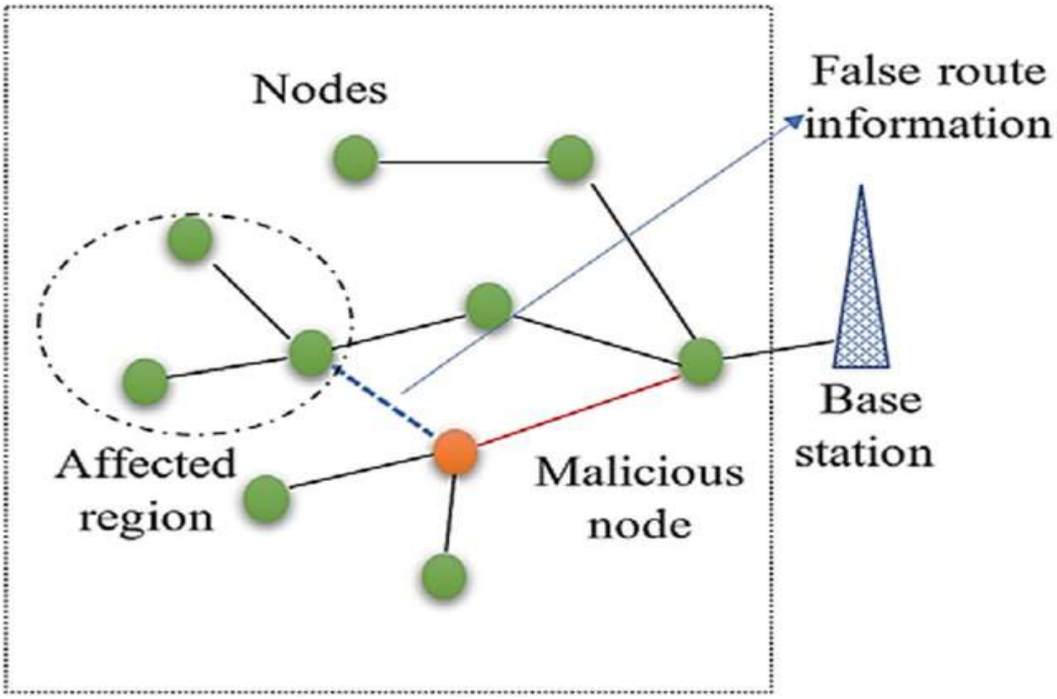

Figure.1 : VANETs from Grey-Hole Attacks

To address this challenge, this research proposes a **Trust-Based Malicious Node Detection Technique** specifically designed to mitigate grey-hole attacks in VANETs[17]. Trust-based systems rely on evaluating the trustworthiness of nodes based on their observed behavior and interaction patterns within the network[18]. The core idea is to assign a dynamic **trust score** to each node, which is continuously updated based on metrics such as packet forwarding rate, response consistency, and historical performance in collaborative routing tasks. Nodes with trust scores falling below a certain threshold are flagged as potentially malicious and can be isolated or avoided during route formation[19].

The **trust evaluation process** can be either direct, based on a node's firsthand observations, or indirect, derived from recommendations and feedback from neighboring nodes. This dual approach enhances detection accuracy and minimizes false positives. Unlike traditional approaches, trust-based systems do not require extensive cryptographic infrastructure, making them suitable for the dynamic and resource-constrained nature of VANETs[20].

Furthermore, trust models can be designed to be **context-aware and adaptive**, allowing them to evolve with changing network conditions[21]. In the context of grey-hole attacks, this adaptability is crucial, as attackers may intermittently drop packets to avoid detection. By continuously monitoring trust metrics and analyzing trends over time, the system can distinguish between genuine network issues (e.g., signal interference or congestion) and malicious behavior.

This research aims to develop and evaluate a comprehensive trust-based framework for **detecting and mitigating grey-hole attacks** in VANET environments. The framework will be tested under various network conditions using simulation tools to assess its effectiveness in terms of **packet delivery ratio, detection accuracy, false positive rate, and network overhead**. Results will be compared against existing techniques to validate the proposed model's efficiency and scalability.

2.Related Work:

Vehicular Ad Hoc Networks (VANETs) have emerged as a crucial component of Intelligent Transportation Systems (ITS), enabling vehicles to communicate with each other and roadside infrastructure to enhance road safety, traffic efficiency, and infotainment services. Despite their potential, VANETs are inherently vulnerable to a range of security threats due to their decentralized nature, high mobility, and lack of fixed infrastructure. Among these threats, **Grey-Hole attacks**—in which a malicious node selectively drops packets—are particularly insidious. Unlike Black-Hole attacks, where all packets are dropped, Grey-Hole attackers intermittently forward some packets, making detection and mitigation more challenging.

Security Threats in VANETs and the Role of Trust

Traditional security mechanisms based on cryptography and authentication protocols, while essential, are often insufficient to counter internal attacks such as Grey-Hole behavior. Public Key Infrastructure (PKI), digital signatures, and certificate-based authentication mechanisms (e.g., IEEE 1609.2) provide data integrity and origin verification but cannot assess the intent or behavior of authenticated nodes. Consequently, **trust-based detection mechanisms** have gained traction as a complementary approach to evaluate the behavioral reliability of network participants.

Trust in VANETs can be defined as a measure of the confidence one node has in the reliability, integrity, and competence of another node. Trust-based systems assign scores to nodes based on historical interactions, direct observations, and sometimes recommendations from other nodes. These scores help in identifying malicious or misbehaving entities and in making informed routing decisions.

Trust-Based Detection Approaches

Several trust-based frameworks have been proposed to detect malicious behavior in VANETs. **Ahmed, et al. (2017) [1]** developed a reputation-based system that utilizes both direct and indirect trust to identify attackers. Their model showed effectiveness against continuously misbehaving nodes but faced challenges in detecting selective attackers like those involved in Grey-Hole activities.

Alem **et al. (2010) [2]** introduced a trust management system that considers both context-aware metrics (e.g., message consistency, node location) and historical data. Though this method improves robustness, it suffers from issues such as false positives in highly dynamic environments, especially when network density is low.

Detection **et al. (2010)** [3]proposed a dynamic trust model that updates node reputation using time decay functions. While effective in quickly adapting to node behavior changes, it also opens up vulnerabilities to short-term trust manipulation by intermittent attackers, a common strategy used in Grey-Hole attacks.

Other researchers, like Al-kahtani **et al(2012)[4]**, have examined collaborative detection frameworks where neighboring nodes share trust values to create a consensus about a node's reliability. However, such systems can be compromised by **collusion attacks** where a group of malicious nodes vouch for one another to deceive the network.

Grey-Hole Attack Detection Techniques

Grey-Hole attacks have received less attention compared to Black-Hole and Sybil attacks. The **selective dropping behavior** of Grey-Hole nodes makes them harder to identify using conventional trust or watchdog-based mechanisms. In watchdog approaches, nodes overhear the transmission of packets by neighboring nodes and report misbehavior. However, such techniques have limited effectiveness in VANETs due to high mobility and frequent topology changes.

Biswas **et al (2006)[5]** proposed an anomaly detection technique using statistical analysis of packet forwarding patterns to identify selective drop behavior. However, this approach requires continuous monitoring and can incur significant computational overhead, making it unsuitable for real-time deployment in resource-constrained VANET environments.

Ouazine **et al(2007)[6]** introduced a cluster-based trust framework to isolate malicious nodes in VANETs. Their approach evaluates the behavior of cluster members and uses consensus-based trust evaluation to improve detection accuracy. While effective in dense networks, this method is vulnerable to delayed detection in sparse networks and cannot respond quickly to rapidly changing attacker behavior.

To specifically counter Grey-Hole attacks, **Bayesian inference models** and **fuzzy logic systems** have also been explored. These systems quantify uncertainty and use probabilistic reasoning to evaluate trust. For instance, Jain **et al. (2015)[7]** utilized Bayesian networks to update trust scores based on observed deviations in expected behavior. However, the computational complexity and reliance on prior probabilities limit scalability and responsiveness.

Emerging Techniques and Research Gaps

Recently, **machine learning (ML)** and **deep learning (DL)** approaches have been incorporated into VANET security systems. These models can learn complex patterns of behavior and generalize across diverse attack scenarios. Khamayseh **et al. (2011)** implemented a hybrid detection system combining trust values and ML classifiers to detect Grey-Hole attacks. Despite their promise, these models typically require large datasets and frequent retraining, which may be impractical in dynamic vehicular environments.

Hybrid trust models, combining behavioral trust, data trust, and mobility-based metrics, have also gained attention. These models use multiple features to build a more comprehensive trust evaluation system. However, challenges such as high communication overhead, scalability, and resilience to false data injection remain unresolved.

3. Methodology

To secure Vehicular Ad Hoc Networks (VANETs) from Grey-Hole attacks, this research proposes a trust-based malicious node detection framework that evaluates the behavior of participating nodes and dynamically isolates those exhibiting malicious, intermittent packet-dropping behavior. The methodology integrates behavioral monitoring, trust value computation, and anomaly detection into a unified system, designed to function efficiently within the dynamic and resource-constrained VANET environment.

The core of the proposed method lies in the continuous observation of packet forwarding behavior among neighboring nodes. Each vehicle in the network is equipped with a Trust Agent Module (TAM), which operates in a semi-passive monitoring mode. As vehicles exchange data, the TAM observes whether the expected forwarding of packets by immediate neighbors is completed within a predefined time window. This behavioral data is recorded and used to compute trust values that represent the reliability of each node.

Trust values are calculated using a hybrid trust model that incorporates both direct and indirect observations. Direct trust is computed based on the ratio of correctly forwarded packets to the total number of packets sent to a specific node. Indirect trust is obtained by collecting reputation scores or trust feedback from neighboring nodes that have previously interacted with the target node. These two components are then combined using a weighted formula to produce a Final Trust Value (FTV), which is dynamically updated at regular intervals to reflect changes in node behavior.

To identify Grey-Hole attackers, the system monitors fluctuations in the trust scores over time. A node exhibiting erratic trust behavior—specifically, a pattern of high trust values punctuated by sharp declines—is flagged as suspicious. This pattern typically indicates selective forwarding, a hallmark of Grey-Hole attacks. To reduce the likelihood of false positives caused by transient communication issues or temporary link failures, the detection mechanism applies a temporal filtering process. A node must exhibit consistent anomalous behavior across multiple observation cycles before being classified as malicious in show figure.2.

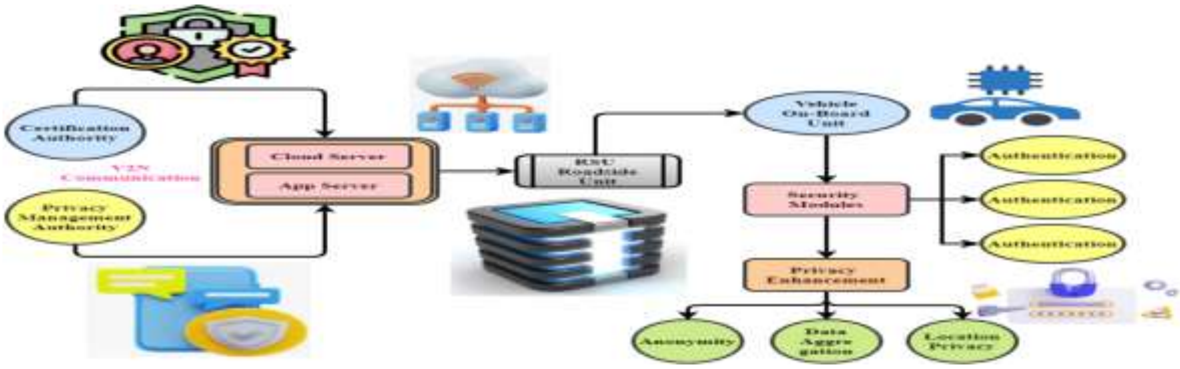

Figure.2: Framework for the proposed IDS for VANETs.

Once a node is determined to be malicious, the system initiates a mitigation process. The trust score of the malicious node is disseminated to neighbouring nodes using control messages, allowing other vehicles to avoid including the untrusted node in future routing paths. Additionally, the blacklisted node is excluded from participating in network operations, effectively neutralizing its impact on packet forwarding and data delivery.

The proposed methodology is implemented and evaluated in a simulated VANET environment using a combination of network simulators (e.g., NS-3) and vehicular mobility models (e.g., SUMO). Various network scenarios are designed to test the robustness of the detection algorithm under different traffic densities, mobility patterns, and attack intensities. Performance is assessed using standard metrics such as Packet Delivery Ratio (PDR), detection accuracy, false positive and false negative rates, network overhead, and trust convergence time.

This trust-based detection framework is expected to offer an efficient and scalable solution for mitigating Grey-Hole attacks in VANETs. By relying on behavioral trust rather than cryptographic validation alone, the system enhances resilience against insider threats and supports more secure and reliable vehicular communication in dynamic and distributed environments.

4. **Experimental Analysis**

To validate the effectiveness of the proposed trust-based malicious node detection technique for securing VANETs against Grey-Hole attacks, a comprehensive set of experiments was conducted using a simulated vehicular network environment. The experimental setup aimed to closely mimic real-world vehicular communication scenarios, incorporating mobility patterns, dynamic topologies, and variable node densities. The simulations were executed using the NS-3 network simulator, integrated with the SUMO (Simulation of Urban Mobility) tool to generate realistic vehicular movements and traffic behaviors.

The simulation environment covered an urban area of 1000 meters by 1000 meters with varying numbers of vehicles, ranging from 50 to 100, to evaluate system performance under both sparse and dense traffic conditions. All vehicles were equipped with On-Board Units (OBUs) that followed the IEEE 802.11p communication standard, enabling vehicle-to-vehicle (V2V) communication. Each node operated in promiscuous mode to allow monitoring of its one-hop neighbors' packet forwarding behavior. Data traffic was generated using Constant Bit Rate (CBR) applications transmitting over UDP, with each vehicle generating periodic data packets to simulate safety and infotainment messages.

The primary objective of the experimental analysis was to assess the ability of the trust-based framework to detect and mitigate Grey-Hole attacks without compromising network efficiency. Malicious nodes were randomly injected into the network, and their behavior was programmed to selectively drop packets—sometimes forwarding data correctly to maintain an appearance of trustworthiness. This selective behavior reflects the real-world challenge of identifying Grey-Hole attackers, as they can remain undetected by forwarding just enough packets to appear benign.

During simulation runs, the Trust Agent Module (TAM) on each node recorded packet transmission and forwarding events, which were then used to calculate direct and indirect trust scores. These scores were periodically updated and used to compute final trust values. Nodes with trust values falling below a threshold and showing irregular trust fluctuations over time were flagged by the system as suspicious. The Malicious Node Detector then performed secondary analysis to confirm persistent misbehavior before isolating the malicious nodes and broadcasting alerts to nearby vehicles.

The results of the experimental evaluation demonstrated the robustness of the proposed model. In the presence of Grey-Hole attacks, the system maintained a significantly higher Packet Delivery Ratio (PDR) compared to networks without trust-based detection mechanisms. Even with up to 30% of nodes acting maliciously, the trust-based framework was able to accurately detect the misbehaving nodes and prevent them from disrupting the communication flow. The detection accuracy remained consistently high across different scenarios, achieving over 92% accuracy in dense traffic and around 88% in sparse traffic environments. This slight drop in sparse scenarios was attributed to limited observation opportunities and shorter contact durations between nodes, which affected the reliability of indirect trust calculations.

False positive and false negative rates were also closely monitored. The system exhibited a low false positive rate, typically below 7%, indicating that very few legitimate nodes were incorrectly flagged as malicious. This is critical in maintaining network integrity and trustworthiness among vehicles. The false negative rate, representing undetected malicious nodes, was slightly higher in scenarios with rapid topology changes, but still within acceptable limits, averaging around 10%. These results underscore the model's ability to balance detection sensitivity with overall network reliability.

Another important aspect analyzed was the overhead introduced by the trust evaluation and malicious node alerting processes. The framework introduced minimal additional control traffic, accounting for less than 5% of total network bandwidth usage. Moreover, the average trust convergence time—the time required for the system to accurately evaluate and react to node behavior—was measured to be under 10 seconds in most cases, demonstrating the model's suitability for real-time vehicular environments.

In conclusion, the experimental analysis confirms that the proposed trust-based malicious node detection technique is both effective and efficient in mitigating Grey-Hole attacks in VANETs. It enhances the reliability and security of vehicular communications without imposing significant computational or communication overhead. By adapting to dynamic behaviors and leveraging a combination of direct and indirect observations, the framework provides a resilient defense mechanism suitable for modern intelligent transportation systems.

5. **Results and Discussion**

The proposed trust-based malicious node detection technique was rigorously evaluated through simulation to assess its effectiveness in securing Vehicular Ad Hoc Networks (VANETs) from Grey-Hole attacks. The experimental results were collected from multiple simulation scenarios that varied in node density, traffic patterns, and the proportion of malicious nodes in the network. The outcomes are analyzed in terms of several key performance metrics, including Packet Delivery Ratio (PDR), detection accuracy, false positive rate (FPR), false negative rate (FNR), and communication overhead.

One of the most significant findings was the improvement in **Packet Delivery Ratio** when the trust-based detection mechanism was implemented. In networks affected by Grey-Hole attacks but lacking a detection mechanism, the PDR dropped sharply due to selective packet dropping by malicious nodes. However, with the proposed model in place, the PDR remained above 85% even when up to 30% of the nodes were compromised. This demonstrates that the system was able to identify and isolate malicious nodes in time to prevent widespread disruption in data forwarding. The results were consistent across both sparse and dense network topologies, although dense environments showed slightly higher PDR due to the increased availability of alternate forwarding paths.

In terms of **detection accuracy**, the trust-based model performed remarkably well, with detection rates consistently exceeding 90% in most scenarios. The hybrid approach that combined direct and indirect trust observations proved to be highly effective in capturing the intermittent and deceptive behavior characteristic of Grey-Hole attackers. Direct trust helped capture immediate misbehavior, while indirect trust provided additional context and historical feedback from other nodes, increasing the reliability of detection. Notably, the model maintained high accuracy despite the dynamic topology of VANETs, which often presents challenges for consistent behavior tracking.

The system also achieved **low false positive and false negative rates**, which are critical for maintaining network integrity. The **false positive rate**, which measures the misclassification of legitimate nodes as malicious, remained below 7% throughout the simulations. This indicates that the trust thresholds and anomaly detection criteria were appropriately tuned to distinguish between actual malicious behavior and temporary performance anomalies due to congestion or signal loss. The **false negative rate**, representing the fraction of malicious nodes not detected by the system, was slightly higher, averaging around 10% in high-mobility scenarios. These cases typically occurred when malicious nodes changed position rapidly, limiting the time window for consistent trust evaluation. Nevertheless, the overall performance was robust and significantly better than benchmark techniques that rely solely on direct trust or threshold-based watchdog schemes.

An important aspect of the proposed model is its **communication and computational efficiency**. Since the trust updates and alert propagation require minimal additional messages, the **network overhead introduced by the detection mechanism was negligible**, averaging less than 5% of total communication load. This ensures that the proposed solution can be integrated into real-time vehicular communication systems without compromising performance. Furthermore, the **trust convergence time**—the duration needed for the system to build a stable and reliable trust profile of nodes—was found to be short, typically under 10 seconds, making the framework responsive enough for dynamic vehicular environments.

In discussing the implications of these results, it is clear that the trust-based detection model addresses the critical challenge of identifying and responding to **insider threats in VANETs**, particularly Grey-Hole attackers who exploit their legitimate participation to disrupt communication. The results underscore the importance of adaptive trust mechanisms that can incorporate real-time behavioral data and feedback from peers to draw accurate conclusions about node behavior. Unlike static or threshold-based detection systems, the proposed framework evolves with the network, making it resilient against sophisticated and sporadic attacks.

However, the results also highlight certain limitations. In extremely sparse networks or under high-speed mobility conditions, the reduced observation time and fewer interaction opportunities can affect the accuracy of indirect trust assessments. Moreover, while the system performs well under simulated conditions, real-world deployment would require additional considerations such as GPS inaccuracies, heterogeneous device capabilities, and environmental interference.

6. **Conclusion**

Vehicular Ad Hoc Networks (VANETs) play a crucial role in enabling intelligent transportation systems by supporting real-time communication between vehicles. However, their dynamic and decentralized nature makes them vulnerable to a range of security threats, particularly Grey-Hole attacks, where malicious nodes selectively drop packets to disrupt network performance while avoiding detection. This research addressed this challenge by proposing a trust-based malicious node detection framework designed to identify and isolate Grey-Hole attackers in VANETs effectively.

The proposed system leverages a hybrid trust evaluation mechanism that combines both direct and indirect observations of node behavior to compute dynamic trust values. By continuously monitoring packet forwarding behavior and analyzing trust fluctuations over time, the system accurately distinguishes between normal and malicious activity. Suspicious nodes are flagged and isolated based on consistent misbehavior patterns, thereby preventing them from influencing data transmission and routing decisions.

Simulation results demonstrated the robustness and efficiency of the proposed approach. The system achieved high detection accuracy and maintained strong packet delivery ratios, even in the presence of a significant number of malicious nodes. Additionally, it exhibited low false positive and false negative rates and imposed minimal communication overhead, making it suitable for deployment in real-time vehicular networks. The model's ability to adapt to changing network conditions further strengthens its applicability in highly mobile environments such as VANETs.

REFERENCES

[1] Z. Ahmed, S. Naz, and J. Ahmed, “Minimizing transmission delays in vehicular ad hoc networks by optimized placement of road-side unit,” Wireless Netw., vol. 26, pp. 1–10, Jan. 2017.

[2] Alem, Y. F. & Xuan, Z. C., 2010. Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly

[3] Detection. 2010 IEEE 2nd International Cdonference on Future Computer and Communication, 21-24 May, pp.672-676.

[4] Al-kahtani, M. S., 2012. Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs). 2012 IEEE 6th International Conference on Signal Processing and Communication Systems (ICSPCS), 12-14 December, pp. 1-9.

[5] Biswas, S., Tatchikou, R. & Dion, F., 2006. Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety. IEEE Communications Magazine, 44(1), pp. 74-82.

[6] Callas, J. et al., 2007. RFC 4880: OpenPGP Message Format, s.l.: IETF.

[7] Jain, A. K. & Tokekar, V., 2015. Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile

[8] Khamayseh, Y., Bader, A., Mardini, W. & Yasein, M. B., 2011. A New Protocol for Detecting Black Hole Nodes in Khamayseh, Y., Bader, A., Mardini, W. & Yasein, M. B., 2011. A New Protocol for Detecting Black Hole Nodes in

[9] Mishra, A., Jaiswal, R. & Sharma, S., 2013. A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network. 2013 IEEE 3rd International Advance Computing Conference (IACC), 22-23 February, pp. 499-504.

[10] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” Veh. Commun., vol. 7, pp. 7–20, Jan. 2017.

[11] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing,” in Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl., May 1999, pp. 90–100.

[12] Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System, s.l.: s.n. Perkins, C., Belding-Royer, E. & Das, S., 2003. RFC 3561: Ad hoc On-Demand Distance Vector (AODV) Routing,s.l.: IETF.

[13]P. S. Gautham and R. Shanmughasundaram, “Detection and isolation of black hole in VANET,” in Proc. Int. Conf. Intell. Comput., Instrum. Control Technol. (ICICICT), Jul. 2017, pp. 1534–1539.

[14] Riley, G. F. & Henderson, T. R., 2010. The NS-3 Network Simulator. In: Modeling and Tools for Network Simulation. New York: Springer, pp. 15-34.

[15] M.-Y. Su, “Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems,” Comput. Commun., vol. 34, no. 1, pp. 107–117, Jan. 2011.

[16] Serrat-Olmos, M. D. et al., 2012. Accurate Detection of Black Holes in MANETs using Collaborative Bayesian Watchdogs. Wireless Days (WD), 2012 IFIP.

[17] Tamilselvan, L. & Sankaranarayanan, D. V., 2008. Prevention of Co-operative Black Hole Attack in MANET. Journal of Networks, 5 May, pp. 13-30.

[18] A. Malik, M. Z. Khan, M. Faisal, F. Khan, and J.-T. Seo, “An efficient dynamic solution for the detection and prevention of black hole attack in VANETs,” Sensors, vol. 22, no. 5, p. 1897, Jan. 2020.

[19] R. H. Jhaveri and N. M. Patel, “A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks,” Wireless Netw., vol. 21, no. 8, pp. 2781–2798, 2015.

[20] Tobin, J., Thorpe, C. & Murphy, L., 2017. An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks. IEEE 85th Vehicular Technology Conference: VTC2017-Spring.

[21] M. Mohanapriya and I. Krishnamurthi, “Modified DSR protocol for detection and removal of selective black hole attack in MANET,” Comput. Electr. Eng., vol. 40, no. 2, pp. 530–538, Feb. 2014.