**Report of my research work done over the past two weeks**

**(From Feb-1 to Feb-15)**

* Professor Johnson Thomas & Professor Park accepted to be part of my thesis grad committee members – I have to update/post it in the study plan.
* **Black Hole Attacks:**

In a black hole attack, a malicious node attracts network traffic by falsely advertising itself as having the shortest path to a destination. Once the traffic is routed through the malicious node, it drops or absorbs the packets, effectively creating a "black hole" where the data disappears without reaching its intended destination.

Here are some key aspects and details about black hole attacks:

1. Motivation:

The primary goal of a black hole attack is to disrupt communication in the network by selectively dropping or absorbing packets, leading to information loss and network degradation.

2. Techniques:

The malicious node may use various techniques to attract traffic, such as falsely advertising a high-quality route, forging routing information, or sending false route reply messages.

3. Routing Protocol Exploitation:

Black hole attacks often exploit vulnerabilities in the routing protocols used in MANETs or WSNs. Commonly targeted protocols include AODV (Ad-hoc On-D Demand Distance Vector), DSR (Dynamic Source Routing), and others.

4. Detection and Prevention:

Detecting black hole attacks can be challenging, as the malicious node may behave normally until it decides to drop packets. Various detection and prevention mechanisms have been proposed, including monitoring packet delivery ratios, analyzing routing table inconsistencies, and using cryptographic techniques for secure communication.

5. Collaborative Approaches:

Collaborative detection approaches involve multiple nodes working together to identify and isolate malicious nodes. This can include reputation-based systems where nodes maintain a reputation score for each neighbor based on their observed behavior.

6. Secure Routing Protocols:

Researchers have also proposed secure routing protocols designed to withstand attacks, including black hole attacks. These protocols often incorporate cryptographic techniques to secure the routing information and prevent tampering.

7. Impact:

Black-hole attacks can have severe consequences on the network, leading to data loss, disruption of communication, and potential denial of service. They pose a significant challenge in securing MANETs and WSNs, where nodes are often resource constrained.

Addressing the security challenges in MANETs and WSNs requires a combination of secure routing protocols, intrusion detection systems, and collaborative approaches to mitigate the impact of black hole attacks and other potential threats.

* **AODV Protocol ( Adhoc On-demand Distance Vector Routing):**

Ad-hoc On-Demand Distance Vector (AODV) is a routing protocol designed for mobile ad-hoc networks (MANETs). MANETs are decentralized networks where nodes communicate with each other directly, without the need for a fixed infrastructure. AODV is specifically designed to provide efficient and dynamic routing in such dynamic and resource-constrained environments. Here are more detailed aspects of the AODV protocol:

1. Route Discovery:

AODV is an on-demand routing protocol, meaning that it only establishes routes between nodes when needed. When a source node wants to send data to a destination and does not have a valid route, it initiates a route discovery process.

2. Route Request (RREQ):

The source node broadcasts a Route Request (RREQ) packet to its neighbors. The RREQ contains information about the source, destination, a unique identifier, and a sequence number. Each node receiving the RREQ checks whether it has a route to the destination or knows a more recent route. If not, it rebroadcasts the RREQ.

3. Route Reply (RREP):

When the RREQ reaches the destination or a node with a fresh route to the destination, a Route Reply (RREP) is generated. The RREP is unicast back to the source along the reverse path of the RREQ. Nodes along this path update their routing tables to establish the route.

4. Route Maintenance:

AODV includes mechanisms for route maintenance. If a link or node along the established route fails or becomes unreachable, the affected node generates a Route Error (RERR) packet. The RERR is then propagated to inform other nodes about the broken link, and affected nodes update their routing tables accordingly.

5. Sequence Numbers:

AODV uses sequence numbers to maintain the freshness of routing information. Each node maintains a sequence number for itself, and these numbers are included in the RREQ and RREP packets. Sequence numbers help in preventing the formation of loops and ensuring the selection of the most recent routes.

6. Hello Messages:

AODV supports the use of Hello messages for link detection and neighbor sensing. Nodes periodically exchange Hello messages to determine the status of their neighbors and update their routing tables accordingly.

7. Loop Avoidance:

AODV employs various mechanisms to prevent the formation of loops in the routing tables. Sequence numbers and the use of a logical time-to-live (TTL) field in the RREQ and RREP packets help avoid routing loops.

8. Optimization:

AODV has been optimized and extended in various ways to address specific challenges and improve its performance in different scenarios. These optimizations include mechanisms to reduce control message overhead, improve route discovery, and enhance overall efficiency.

AODV is widely used in MANETs due to its simplicity, efficiency in route discovery, and ability to adapt to dynamic network conditions. However, like any protocol, it has its limitations, and researchers continue to explore enhancements and alternatives to address specific challenges in MANET environments.

* **Read 2020 conference paper --**

***“Security methods against Black Hole attacks in Vehicular Ad-Hoc Network”***

**Algorithms or Methods Discussed:**

A. Algorithm against Black Hole attackers – SIN (So-called Intelligent Nodes)

B. Upgraded version of Ad-Hoc Distant Vector Routing (AODV)

C. Permutation Based Acknowledgment (PBAck)

D. Secret Ad-Hoc Distant Vector Routing (SAODV)

E. Intrusion Detection using Anomaly Detection (IDAD)

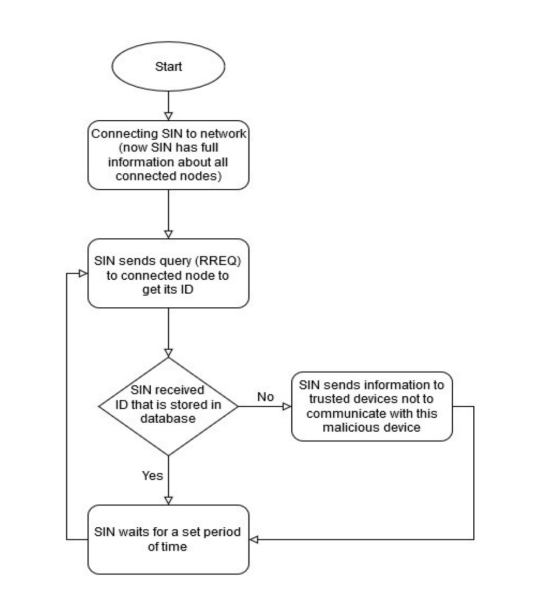
Then compared SIN with other algorithms.

**Brief Summary:**

This paper discusses security methods against Black Hole attacks in Vehicular Ad-Hoc Networks (VANETs). VANETs are susceptible to Black, Worm, and Gray Hole attacks due to the broadcast nature of the wireless medium and a lack of authority standards. A Black Hole attack occurs when a malicious node falsely claims to have the shortest route to a destination node, leading to dropped or redirected data packets without the source node's knowledge. The consequences of such attacks can be severe, impacting network infrastructure and potentially endangering lives.

To prevent Black Hole attacks, the paper explores methods such as Secret Ad-Hoc Distant Vector Routing (SAODV) and Intrusion Detection using Anomaly Detection (IDAD). SAODV extends AODV by verifying secure paths with secret codes, while IDAD uses anomaly detection to identify malicious activities. Additionally, an algorithm involving intelligent nodes (SINs) is proposed to detect and isolate Black Hole attackers in VANETs.

Overall, the paper aims to investigate and compare these methods to enhance security and prevent Black Hole attacks in VANETs, emphasizing the importance of safeguarding networks against various forms of attacks to ensure safe and efficient communication among vehicles.



*Fig: Algorithm to detect Black Hole attackers*

**About Black Holes as per the paper information**

Black Hole attacks in Vehicular Ad-Hoc Networks (VANETs) involve a malicious node falsely claiming to have the shortest route to a destination node. Here is how Black Hole attacks work and their potential consequences:

**1. How Black Hole Attacks Work:**

- The malicious node advertises itself as having the most efficient path to the destination node.

- When other nodes in the network send data packets intended for the destination, they are redirected to the malicious node.

- The malicious node can then drop the packets, launch denial of service attacks, or even act as a man-in-the-middle to intercept and manipulate the data.

- By disrupting communication and misleading nodes about the optimal route, the attacker can cause chaos and compromise the integrity of the network.

**2. Potential Consequences of Black Hole Attacks:**

*- Disruption of Communication:* Black Hole attacks can lead to the disruption of communication between legitimate nodes, preventing data from reaching its intended destination.

*-Denial of Service:* By absorbing or dropping data packets, Black Hole attackers can launch denial of service attacks, impacting the availability and reliability of the network.

*- Compromised Data Integrity:* Manipulating or intercepting data packets can compromise the integrity and confidentiality of the information being transmitted.

*- Endangering Lives:* In the context of VANETs, where communication is crucial for traffic safety and efficiency, Black Hole attacks can potentially endanger lives by disrupting critical information sharing among vehicles.

Overall, Black Hole attacks pose a significant threat to the security and functionality of VANETs, highlighting the importance of implementing robust security measures to detect and prevent such malicious activities.

* **Read 2021 conference paper --**

***“A Dual Approach for Preventing Blackhole Attacks in Vehicular Ad Hoc Networks***  ***Using Statistical Techniques and Supervised Machine Learning”***

**Brief Summary:**

This paper discusses a dual approach for preventing blackhole attacks in Vehicular Ad Hoc Networks (VANETs) using statistical techniques and supervised machine learning.

The study compares different classifiers such as Naive Bayes, k-Nearest Neighbor, Logistic Regression, Support Vector Machine (SVM), and Gradient Boosting.

Among these classifiers, SVM and Gradient Boosting demonstrate high accuracy (over 98%), F1-score (over 95%), and ROC AUC score (over 97%) in detecting blackhole attacks.

Gradient Boosting, as an ensemble learner, shows slightly better performance than SVM. The paper also explains the concepts of Gaussian Naive Bayes, Logistic Regression, and Gradient Boosting classifiers in the context of VANET security.

Additionally, it provides insights into simulation parameters, dataset characteristics, and evaluation metrics like accuracy, recall, precision, F1-score, false positive rate, and ROC AUC score. The results indicate that the proposed model is scalable and effective in detecting malicious vehicles in VANETs.

**Some more info as per paper:**

Statistical modeling and machine learning techniques work together to prevent blackhole attacks in VANETs by leveraging the strengths of each approach:

1. **Statistical Modeling**: Statistical techniques, such as feature selection using analysis of variance (ANOVA), help in identifying the most relevant features that can distinguish between normal and malicious behavior in VANETs. By selecting the best features, statistical modeling reduces the dimensionality of the data and improves the efficiency of machine learning algorithms.
2. **Machine Learning**: Machine learning algorithms, such as Support Vector Machine (SVM), Gradient Boosting, Naive Bayes, k-Nearest Neighbor, and Logistic Regression, are used to classify incoming traffic flows, detect malicious vehicles, and prevent blackhole attacks. These algorithms learn patterns from the data and make predictions based on the identified features.
3. **Combining Statistical Modeling and Machine Learning**: By combining statistical modeling for feature selection and machine learning for classification, the system can effectively differentiate between normal and malicious behavior in VANETs. Statistical techniques help in preprocessing the data and selecting relevant features, while machine learning algorithms utilize this processed data to build models for detecting and preventing blackhole attacks.

Overall, the integration of statistical modeling and machine learning techniques provides a comprehensive approach to enhancing security in VANETs by accurately identifying and mitigating threats posed by malicious vehicles, such as blackhole attacks.