Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Analysing Degradation Of Network Performance In Manet Due To Presence Of Malicious Nodes

Prolay Ghosh[1], Dr. Nisarg Gandhewar[2]

[1] Research Scholar, Department of Computer Science and Engineering, Dr. A.P.J Abdul Kalam University, Indore, M.P.

[2] Research Guide, Department of Computer Science and Engineering, Dr. A. P. J. Abdul Kalam University, Indore, M.P.

ABSTRACT

Mobile Ad hoc Networks (MANET) are networks without a physical infrastructure that offer several wireless hops between nodes. Military and emergency situations, when a permanent infrastructure is not necessary, are where MANET is mostly used in real-time environments. It is a temporary communication infrastructure network for efficient node-to-node communication with few setup requirements. One of the main issues in MANET is security. In a MANET setting, malicious nodes reduce network performance. The mobile ad hoc networks (MANETS) are multi-hop, decentralized networks in which intermediary nodes act as routers to send data packets to their intended locations. Rough set theory is used in this study to identify malicious nodes. The malicious node is located with the aid of the route cache table using the transmission history. Every node in the network keeps track of its neighboring node's transmission history and cache table. Based on measured transmission parameters, such as packet delivery ratio, throughput, end-to-end latency, number of dropped packets, and error rate the node's transmission history is determined. According to the findings of our experiment, the rough set-based strategy boosts network capacity such as packet delivery ratio and reduces end-to-end latency and throughput.

Keywords: Network, Security, Node, Malicious, Rough set.

I. INTRODUCTION

As seen in figure 1, mobile ad-hoc networks are made up of various wireless mobile devices called nodes. These networks lack a centralised administrative structure and a permanent infrastructure. Resource limitations, changeable topology, and openness to wire media are characteristics of MANETs. Wireless networks do, however, contain a variety of weaknesses that might be used by hackers to enter the network and steal or alter data.

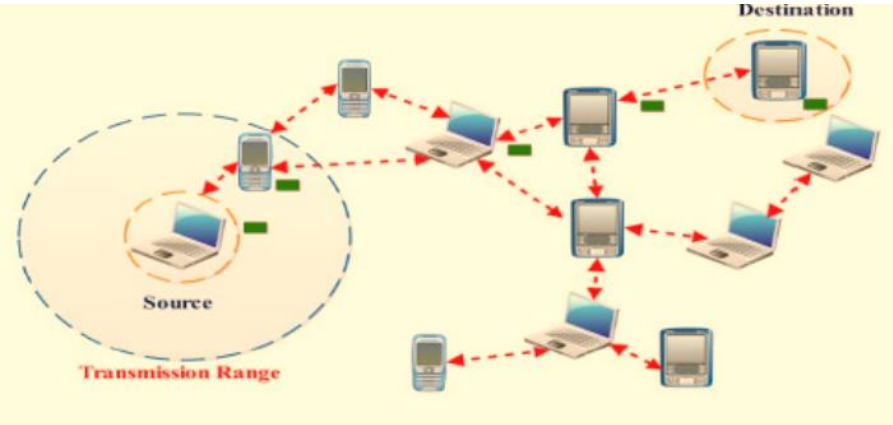

Figure 1: MANET architecture

This type of network is ideal for mission-critical applications like disaster relief, military operations, and counterterrorism when there is no pre-deployed communication infrastructure. Mobile ad hoc networks are susceptible to a variety of passive and active assaults due to their inherent characteristics of missing any centralised access control, secure borders (mobile nodes are free to join, leave, and move inside the network), and limited resources. Protection of the network layer against various active routing attacks is one of these issues' most crucial security concerns. In this study, two different routing attacks—the passive Black Hole Attack and the active Black Hole Attack—that display improper packet forwarding behaviour are discussed. In a black hole attack, a malicious node (also known as a black hole) responds to each request for a route by making the untrue assertion that it already has a fresh enough routes to the desired location. This causes every network request to be sent to the rogue node, which dumps them all.

II. SECURITY THREATS IN MANETS

In contrast to fixed hardwired networks with physical security at firewall and gateways, an adhoc networkcan be attacked from any angle at any node. Overall, it means that every node needs to b e prepared to facean attacker, whether they come directly or indirectly.

Attacks that are malicious might come from both within and outside the network. Large adhoc networks make it challenging to track a single node, making it riskier and more challenging to identify assaults coming from a node that has been compromised.

Overall, it means that each node should be ready to operate without instantly putting its faith in another node. High availability should be attained via a distributed architecture. This is so that the entire network won't be seriously attacked if the central entity is employed in the security solution and suffers attack.

The sorts of current assaults and their applicable counter measures are as follows:

Black hole attack: Make H a malicious node. When H gets a route request, it instantly replies with a route reply that builds the data and may e sent via the quickest way. As a result, H –>S

replaces Route Reply after S gets it. The information is then delivered to H by S.

Neighbor attack : Both the black hole attack and the neighbour attack stop the data from reaching its target. However, the nearby attacker fails to intercept and seize the data packets coming from the source node. As soon as the bogus messages are sent, it exits the settings.

Wormhole attack: Two malicious nodes communicate privately with one another using a shared link. One node collects network traffic data and transfers it immediately to another node.

Warm hole has the ability to eavesdrop on traffic, purposefully lose packets, and launch man-in-the-middle attacks against network protocols.

DoS (Denial of Service) attack –

A DoS attack occurs when a malicious node compromises the network bandwidth. The attacker inserts packets into the network in order to make use of valuable network resources like bandwidth or to make use of node resources like memory or processing power. The routing table overflow attack and the energy consumption attack are specialized examples of the DoS attack.

Information Disclosure Attack –

This attack targets the network's privacy standards. A malicious node will release sensitive data to untrusted nodes, such as routing locations, node status, secret keys, and passwords.

Rushing attack - This attack targets on-demand routing systems that employ similar suppression at every node. The source nodes send out the RREQ in order to discover routes to the destinations. Only the first nonduplicate packet is processed by each intermediate node, and all subsequent duplicate packets are discarded. Attackers that are moving swiftly can forward these packets by circumventing parts of the routing procedures.

They may access the forwarding group as well.

Jellyfish attack – A malicious node broadcasts and receives PREQ and PREP as usual. However, it delays the data packets without any justification for a while before forwarding. It is challenging to carry out this kind of attack because the node must first breach the forwarding group. The effect on the network is likewise reduced it there are fewer malicious nodes.

Byzantine attack – This type of attack is also known as an impersonation attack since a malicious node may impersonate a legitimate node. In order to update an anomaly in the routing database, it also transmits bogus routing information. Additionally, an attacker might get access to resources and sensitive data without authorization.

Blackmail attack –

This attack targets routing protocols that employ tools for identifying malicious nodes and broadcast messages that attempt to blacklist the offender. An attacker might extort a genuine node by adding additional legitimate nodes to their blacklists. Therefore, in certain paths, the nodes may be avoided.

III. PROPOSED ROUGH SET THEORY SCHEME OF MALICIOUS NODE IDENTIFICATION IN MANET

DSR Cache Table

A cache table is a data structure that keeps track of each node's routing data, which is helpful for updating the cache. The size of a cache table can grow as new routes are found and shrink as old routes are eliminated; it has no maximum capacity. A cache table entry has four fields: Route, Source Destination, Data Packets, and Reply Record. The linkages starting from the current node to a destination or from a source to a destination are stored in the Route field. It is the pair consisting of the source and destination. Data Packets: It logs if data packets have been transmitted by the current node. Reply Record: There is no upper limit on the number of entries that may be made in this field. Caches' responses offer two performance benefits. They first decrease the latency of route finding. Second, the route query flood will reach every node in the network if caches don't respond (request storm).

Route Cache

In the DSR protocol, all routes learned from the source node to the destination are stored in the route cache in order to prevent needless route finding. As a result, the cache will operate according to the network's existing topology. Since restarting a route discovery procedure in on-demand routing protocols consumes a lot of time, battery life, and bandwidth due to network flooding, it might take a very long time before the first data packet is transferred. An effective route cache implementation is crucial for protocol speed. To find the broken links when an invalid route cache is utilised, additional traffic overheads and routing delays are incurred. The purging of the cache item after a certain Time-to-Live (TTL) period is one method for reducing the impact of an invalid route cache. If the TTL is set too low, it is probable that legitimate routes may be ignored, which might cause significant routing delays and traffic overheads as a result of the fresh route search. To prevent needless route discovery for commonly used routes, the routes are kept in the cache. DSR has two different types of caches. I Path cache: The route cache stores the whole path or all destinations. (ii) Link cache: This is what happens when a node adds each link to a graph of links by caching them separately. The figure 2 displays the node environment.

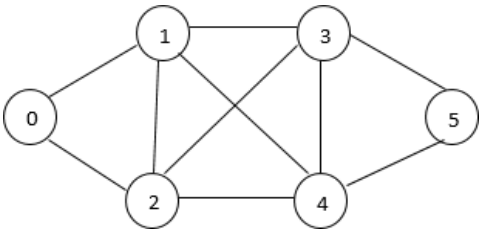

Figure 2 Node Environment

6: 0-1-2-4-5, Path 7: 0-1-2-3-5, Path 8: 0-1-2-3-4-5, Path 9: 0-2-4-5, Path 10: 0-2-4-3-5, Path 11:

0-2- 3-5, Path 12: 0-2-3 Path cache structure: Path 1: 0-1-3-4-5, Path 2: 0-1-3-5, Path 3: 0-1-4-5, Path 4: 0-1-4-3-5, Path 5: 0-1-2-4-3-5, Path -4-5, Path 13: 0-2-1-3-5, Path 14: 0-2-1-3-4-5, Path 15: 0-2-1-4-3-5, Path 16: 0-2-1-4-5.

The route cache will save the path from source 0 to destination 5, much like in the path cache structure. Node 0 will alert the source and the other node via node 3 in this scenario when a misbehaving node is in the path as node 4 leaves the network. The route cache item will be updated with the new path as in the path cache structure when the source discovers a new path to a destination via another node 3.

Transmission Node's metrics

Make a network simulation with a node in it. Based on node performance, a node's transmission metrics are calculated. On the basis of transmission history, one may determine the node's performance. Following is a calculation of transmission history.

Ratio of packet deliveries: The ratio between the number of packets transmitted from the application layer and the number of packets actually received at the destination nodes is shown by the packet delivery ratio.

End-to-end delay: End-to-end refers to an average measurement of performance between network nodes. It involves both the sources and the receivers.

Throughput: Throughput essentially counts the number of successfully delivered packets over the whole simulation. By dividing the total number of packets received by the whole simulation duration, it is computed.

Number of dropped packets: Data packets created from sources that were not delivered to their destinations.

Error rate: Error rate is determined by dividing the number of data packets created by those that were actually received.

Nodes 0 to 5's transmission and metrics are computed at various speeds, including 2, 4, 6, 8, and 10 ms.

The table 1- 6 has the computed sizes.

Table 1 Transmission history of node 0 runs with different speed

Speed @ ms	Packet delivery ratio	End-to-End delay	Throughput	Number of dropped packet	Error Rate

@2	99.9741	15.588	754.81	0	1
@4	98.5052	17.305	751.49	12	0.9896
@6	98.0069	20.918	752.50	10	0.9845
@8	98.0003	25.417	755.88	15	0.9792
@10	98.5787	20.039	753.72	20	0.9882

Table 2 Transmission histories of node 1 runs with different speed

Speed @ ms	**Packet delivery ratio**	**End-to-end delay**	**Throughput**	**Number of dropped packet**	**Error Rate**
@2	99.9329	21.729	755.81	12	0.998
@4	99.0007	17.871	752.78	15	0.989
@6	98.7241	24.091	755.89	16	0.991
@8	98.0001	23.598	752.87	20	0.974
@10	98.8439	39.729	753.71	25	0.979

Table 3 Transmission history of node 2 runs with different speed

Speed @ ms	**Packet delivery ratio**	**End- to- end delay**	**Throughput**	**Number of dropped packet**	**Error Rate**
@2	92.208	27.205	755.78	15	0.991
@4	94.589	30.441	755.91	20	0.941
@6	94.211	32.998	752.53	22	0.839
@8	94.001	33.389	753.67	25	0.979
@10	94.232	38.341	751.61	20	0.101

Table 4 Transmission history of node 3 runs with different speed

Speed @ ms	Packet delivery ratio	End-to-end delay	Throughput	Number of dropped packet	Error Rate
@2	85.2158	52.690	755.78	20	0.582
@4	80.0011	50.989	752.91	15	0.989
@6	82.5532	35.445	753.61	16	0.839
@8	80.5761	57.009	752.53	50	0.979
@10	80.0005	68.115	750.61	11	0.111

Table 5 Transmission history of node 4 runs with different speed

Speed @ ms	Packet delivery ratio	End-to- end delay	Throughput	Number of dropped packet	Error Rate
@2	80.211	66.006	750.59	15	0.988
@4	77.479	65.411	750.88	50	0.980
@6	77.495	62.251	751.59	40	0.103
@8	75.831	80.001	752.78	60	0.027
@10	70.759	72.8883	753.31	52	0.008

Table 6 Transmission history of node 5 runs with different speed

Speed @ ms	Packet delivery ratio	End-to- end delay	Throughput	Number of dropped packet	Error Rate
@2	99.929	15.589	755.81	2	0.991
@4	98.001	20.918	751.50	4	0.942
@6	98.838	25.424	752.51	12	0.843
@8	98.726	17.301	753.71	8	0.979

@10	99.011	30.045	755.79	20	0.986

Information System of Rough Set Theory

Rough set theory

The mathematical method known as rough set theory, which Pawlak introduced in 1982, deals with ambiguity and uncertainty. Based on the connection of indiscernibility, its notions and operations are defined. According to this approach, a data collection is represented as a table, with each row standing in for a particular instance, thing, example, item, or element. An attribute that can be measured for an element is shown in each column. Information systems is the name given to this data table.

Information System

A table with each row representing an item and each column representing an attribute may be used to represent an information system. That is quantifiable for each thing. An information system is essentially a pair S = (U, A), where U is a non-empty finite collection of objects known as the universe and A is a non-empty finite set of characteristics such that a: U Va for every a ∈ A . The set Va is referred to as the value set. A decision system communicates practically all of the model's information. The same or undetectable items may occasionally appear many times in the data table, or some of the features may be unnecessary. Equation (1) can be used to represent this.

$$IND(B) = \{(X, X') \in U2 | \forall a \in B\ a(x) = a(x')\} \quad (1)$$

Where IND(B) is referred to as the B-indiscernibility relation and is an equivalence relation. Lower and higher approximations can be used to do a rough set analysis. This has the following definitions.

Lower approximation

$$B*(X) = \{X \in U: B(X) \subseteq X\} \quad (2)$$

Upper approximation

$$B*(X) = \{X \in U: B(X) \cap X \neq \phi\} \quad (3)$$

Where B ⊆ A and X ⊆ U. By creating the lower approximation and upper approximation specified in (2) and (3), we may approximate X using only the information provided in B. (3). Rough sets cannot be described using available information due to the granularity of the knowledge. As a result, we connect two crisps, referred to as the lower and higher approximations, with each rough set. All items that unquestionably belong to a set make up the

lower approximation of a set. Any rough set has a non-empty set border area, which is the difference between the upper and lower approximations. Numerical characteristics of rough sets can be expressed by the coefficient as in the equation (4).

$$\alpha_B(X) = \frac{|B_*(X)|}{|B^*(X)|} \quad (4)$$

where |X| denote the cardinality X = ϕ. If αB (X) = 1, the set X is crisp with respect to B and ifαB (X) < 1, the set X is rough with respect to B.

Minimal reducts are a kind of conditional attribute subsets that occasionally retain the universe's division into portions. The discernibility matrix function, which may be defined in equation 5, can be used to find such reductions:

$$Cij = \{a \in A | a(xi) \neq a(xj)\} \text{ for } i, j = 1 \ldots \ldots n$$

$$a1 * \ldots \ldots . am * = \Lambda\{V\, Cij * | 1 \leq j \leq i \leq n, Cij \neq \emptyset \quad (5)$$

where $C_{ij}^* = \{a * | a \in Cij\}$. Also we can measure the significance of the approximate reduct and the effect on the data set after dropping that particular attribute by the formula in equation (6)

$$\propto_{(C,D)} = 1 - \gamma(C - \alpha, \frac{D}{\gamma\, C,D} \quad (6)$$

In Table 7, the information system is displayed. Where each column denotes a property and each row denotes an object. The average values of the nodes' behavior are shown in table 7 below.

Table: 7 Average values of nodes based on the transmission history runs with different speed

Nodes	Packet delivery ratio	End-to- end delay	Throughput	Number of dropped packet	Error Rate
0	98.6119	21.79	753.690	10.5	0.984
1	98.9033	25.37	754.131	14.0	0.986
2	93.8501	32.46	753.900	17.0	0.771
3	81.6689	45.77	753.092	18.6	0.705
4	76.3569	69.29	751.848	36.1	0.416

5	98.9005	21.88	753.886	16.4	0.948

Derive IF-THEN decision rules from average values of all the nodes based on the transmission history runs with different speed.

If Packet delivery ratio>= 95 and then decision=high

Else if packet delivery ratio>= 81 then decision =medium

Else if packet delivery ratio≤80 then decision=low

If end-to-end delay≤45 then decision=low

Else if end-to-end delay>50 then decision=high

If Throughput>753 then decision=high Else if throughput<750 then decision=low

If Number of dropped packet<=10 then decision=low

Else if number of dropped packet<=20 then decision=medium Else if number of dropped packet>25 then decision=high

If error rate≤0.984 then decision=low

Else if error rate=0.986 then decision=medium Else if error rate=0.416 then decision=high

Table 8 Data Set

Nodes	PDR	End-to- End delay	Throughput	No. of Dropped Packet	Error Rate	Decision
0	H	L	H	L	L	GOOD
1	H	L	H	L	M	GOOD
2	H	L	H	M	L	GOOD
3	M	L	H	L	L	GOOD
4	L	H	L	H	H	BAD
5	H	L	H	L	L	GOOD

The above rules are used to classify the nodes behavior such as good or bad. If PDR=High/medium, End-to-End delay=Low, Throughput=high, No. of dropped

packet=Low/medium, error rate=Low/medium then decision=Good. Else if PDR=Low, End-to-End delay=high, Throughput=Low, No. of dropped packet=High, Error Rate=High then decision=Bad.

Node Classification Using Rough Set Theory

A node's performance characteristics, such as its packet delivery ratio, end-to-end latency, throughput, number of dropped packets, and error rate, are used to determine if it is a good node or a bad node. The classification of various nodes is shown in Table 8, where H stands for High, M for Medium, and L for Low.

Analysis of Data Using RSES

RSES (Rough Set Exploration System) is used in this dissertation to generate decision rules, which are then applied to a network scenario featuring malicious nodes to identify them. The RSES toolbox for table data analysis uses techniques and algorithms from the field of rough sets. In order to perform our suggested effort to identify the malicious nodes, we will make sure to take the following precautions.

Procedure:

Step1: Load data to the RSES.

Step2: Find the Reduct.

Step3: Derive the Decision rules.

Step4: Use the Classifier known as Decision trees to learn from the training data set.

Step 5: Build the confusion matrix.

Step6: Apply the derived the decision rules to detect the malicious nodes

Malicious Node Identification

In order to categories the nodes according to the decision criteria, the average value of the transmission metrics is taken into account. The properties of each node, whether good or negative, are described by the categorized nodes. Rough set theory is employed to locate the problematic nodes in the network, and various simulations are taken into account at various speeds. The network's malicious nodes are located, and their presence in the path cache is eliminated. The routing mechanism makes advantage of the updated path cache tables. The network's malicious nodes are located using the technique listed below.

Identification of malicious nodes process:

Step 1: create a network simulation with 6 nodes.

Step 2: To find the transmission metrics of a node such as

Packet delivery ratio:

PDR = [(No. of packets Received |No. of packet send)]X100

End-to-End delay:

delay = ∑(arrive time − send time) / ∑ No. of Connections

Throughput:

Throughput = (Received size|start time − stop time)X8/100

Number of dropped packet:

NDP = ∑ Dpackets

Error rate of node:

Error Rate = $\frac{Received\ Packet}{Generated\ Packet}$

Step 3: Perform the simulation with different speed for every node to calculate the transmission metrics of an each node.

Step 4: Derive decision rules based on the transmission metrics Step 5: classify the node whether good or bad, based on the rule.

Step 6: Generate the information table from the transmission metrics table and apply rough set theory to identify the malicious node

Step 7: Remove the malicious node in the cache table and update the cache table. Step 8: Perform the routing process.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

Simulation Environment

A discrete event driven simulator called Network Simulator (NS2) was created at UC Berkeley. The VINT project includes it. Supporting networking research and instruction is the aim of NS2. It is appropriate for creating new protocols, contrasting various protocols, and analysing traffic.

The development of NS2 is a team effort. It is open source and freely available. NS2 is used, maintained, and developed by several institutions and individuals working in development and research.

Table 9 Simulation Environment

Simulation Parameters	
Routing Protocols	DSR
Simulation Time	500 sec
Number of Nodes	6
Simulation Area	1500 X 1500
Pause tine	20 sec
Traffic Type	CBR
Packet Size	512 Bytes
Rate	10 packets/sec

Six wireless mobile nodes are used to create the simulation environment. They are distributed evenly throughout a 1500 x 1500 metre area and move about in a mobile ad hoc network for 500 seconds. The dynamic Source Routing protocol is set up to execute on each mobile node in the network (DSR). The studies presented in this paper make advantage of constant bit rate (CBR) traffic sources. Table 9 lists the simulation parameters.

Performance Metrics

To correspond to the special distinctiveness and recital of network following metrics are used in our simulation:

- Throughput: It basically measures the successful packet delivery over the entire simulation. It is calculated by dividing the total packets received by the total simulation time. Throughput = Pr / (T2 - T1). Where, Pr is total data size received, T1 is the start time and T2 is the stop time of simulation.

- Packet Delivery Ratio: PDR is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. A high PDR is desired in

a network. PDR = (Pr / Ps) * 100 Where, Pr is total packets received and Ps is the total packets sent.

- Average end-to-end Delay: The packets end-to-end delay is the average time that packets have to pass through the network. It represents the reliability of routing protocols. Delay = (T2 – T1) where, T2 is receive time and T1 is sent time.

V. RESULT OF THE STUDY

Performance analysis of existing and proposed work is shown in the figure 3 and table 10.

Table 10: Performance analysis

Analysis	Packet delivery ratio (%)	Throughput (kpbs)	End-to- End Delay(ms)
Existing	97.011	753.88	20.50
Proposed	99.749	250.49	15.27

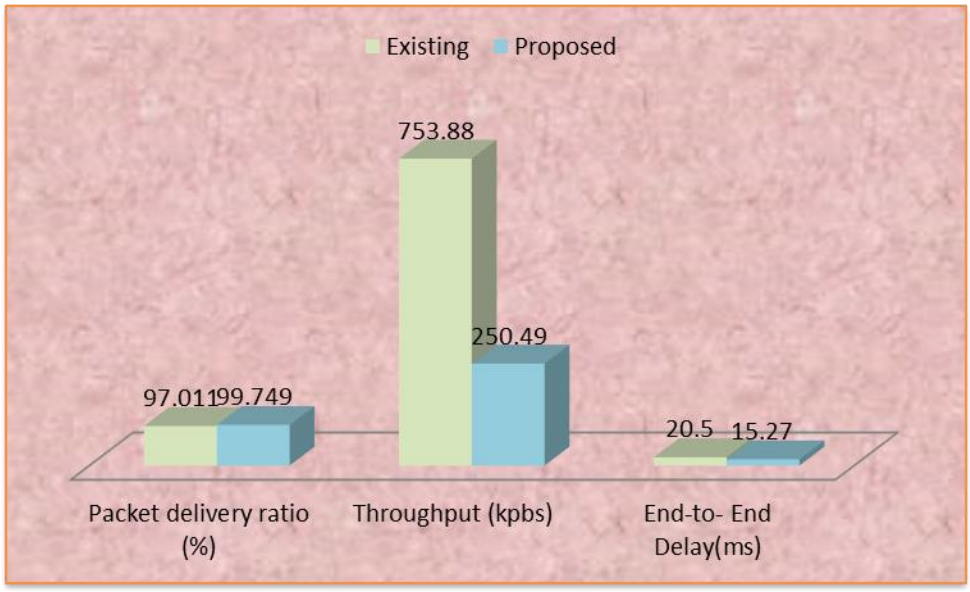

Figure 3: Performance analysis

IV. CONCLUSION

Research and development in the field of security are ongoing. Due to the dynamic nature and

network limitations of ad hoc networks, configuring security mechanisms might be difficult. This paper illustrates how network performance has been severely harmed by packet dropper nodes. The malicious node is located with the aid of the route cache table using the transmission history. Every node in the network keeps track of its neighbouring node's transmission history and cache table. Rough set theory is used to categorise the nodes as excellent or bad based on their transmission history. By maintaining the division of the universe of discourse and generating the decision rules, rough set approaches assist in eliminating the extraneous qualities and offer the reduct set of attributes. The packet forwarder selects the quickest path and an alternate path. As a result, we were able to successfully inject, identify, and prevent packet-dropping nodes from the DSR's path. Since a path cache has been constructed, route breakdown is readily recoverable. This technique has a low false detection rate and little network overhead, among other benefits. Simulation results reveal that following the preventive mechanism, throughput and end-to-end latency have both improved.

Due to its dynamic nature, ad hoc networking is an active and difficult topic of computer science study. Adhoc network, then, has a number of vulnerabilities that need to be investigated and a lot of other problems that need to be resolved. Our next research will focus on other mobile and ad hoc network vulnerabilities. In order to detect the malicious node in the network, we will also attempt to combine this suggested method with additional mechanisms including neural networks, fuzzy sets, and hybrid models.

REFERENCES: -

[1] Jamal, Tauseef & Butt, Shariq. (2018). Malicious node analysis in MANETS. International Journal of Information Technology. 11. 10.1007/s41870-018-0168-2.

[2] Panchapakesan, Ashok. (2017). IDENTIFICATION OF MALICIOUS NODES IN MANET BASED ON NODE GROUPING. International Journal Of Advance Research And Innovative Ideas In Education. 3.

[3] Shahjahan, A. and Parma N.,(2016) “Comparative performance analysis of AODV and DSR routing protocols under wormhole attack in mobile ad hoc network on different node's speeds”, International Conference on Computing Communication and Automation (ICCCA).

[4] Gorine, H. & M.Ramadan Elmezughi., (2016) “Security Threats on Wireless Sensor Network Protocols,” 18th International Conference on Cryptology and Network Security, Kuala Lumpur, 18- 19 August 2016.

[5] Rajeswari, A. & Kanagasabai, Kulothungan & Ganapathy, Satish & Arputharaj, Kannan. (2016). Malicious Nodes Detection in MANET Using Back-Off Clustering Approach. Circuits and Systems. 07. 2070-2079. 10.4236/cs.2016.78180.

[6] Khan, Muhammad Usman & Khan, Mohammad Zunnun & Shoaib, Mohammad. (2014). Detection of Malicious Node in MANET: issues and Challenges on Intrusion Detection.

[7] Kaur, H., Bala, M. and Sahni, V., (2013) "Study of Black Hole Attack using different routing protocols in MANETs." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), 2(7).

[8] Gagandeep, A. & Kumar, P., (2012) "Analysis of Different Security Attacks in MANETs on Protocol Stack" International Journal of Engineering and Advanced Technology (IJEAT), 1(5), pp.269-275.

[9] Kavitha, T. Sridharan, D., (2010) "Security vulnerabilities in wireless sensor networks: A survey". Journal of information Assurance and Security, 5(1), pp. 31-44.

[10] Khokhar Rashid Hafeez, Ngadi Md Asri and Mandala Satria (2008) International Journal of Computer Science and Security 2(3):18-29.

[11] Bingwen He, Hägglund Joakim and GuQing (2005) "Security in Adhoc Networks", An essay produced for the course Secure Computer Systems HT2005 (1DT658)