Security Enhancing based on Node Authentication and Trusted Routing in Mobile Ad Hoc Network (MANET)

M. Venkat Das[1*], P Premchand[2] and L R Raju[3]
Research Scholar, Dept of CSE, UCEOU, Hyderabad
Professor, Dept of CSE, UCEOU, Hyderabad
Assistant Professor, Dept of CSE, Matrusri Engineering College, Hyderabad

Abstract

In theMobile Ad HocNetwork, identifying trusted nodes for secure communication is a key challenge. Node compromises a service and leads to ambiguity in the behaviour of a node in the network. Node authentication and trust level calculation will enhance the security aspect of MANETs. Thispaper proposes enhancing security based onthe "Node Authentication and Trusted Routingapproach (NATR)". NATR aims to avoid abnormal node interference in MANET. There through improved security and output data delivery. NATR calculates the predictability of the node by evaluating the three most common actions performed by a node in the connection process. Node licensing is a key aspect of evaluating custom network security. In this method, we monitor the Success rate of RREQ, Success rate of RREP, and Data Success rate node trust. The reliability of data delivery is measured bythe successfuldelivery of packets and theloss or drop of packets. The experimental results showthere is a 25% increase in package delivery and a 40% decrease in overhead for routing. NATR is compared with SAR TMS, and AODV to assess efficiency in Adhoc networks.

Keywords: ***Trust Computation, Trust Level, Security, MANET***

1.Introduction

A MANET with many wireless devices that are proficient in interacting with any network infrastructure or centralized management. In order to enable multi-hop communication between non-adjacent nodes, the previous node should act as a router. for an open and dynamic environment, and shared or cooperative channels and other resources, MANETs are scarce resources and vulnerable to security attacks than conventional wireless networks. This limitpresents a huge challenge for find and deploy trusted nodes and providing secure communication over the MANET.

Many of the frameworks in these frameworks [1], [2] and [3], [4], [5] are provided in relational and reliable computation-based securities, which are limited for limited resource communication. Resource communication is more effective. It reflects the correlation of managing reliable communications with reliable nodes that operate reliable nodes and more reliable nodes from specific nodes.

To achieve benchmark performance continuously in thissituation, routing technology must remain firm against this dynamic environment format, and node mobility may also result in the loss of existing links, so new ways must be sought to overcome communication disruptions. A faulty node attempts to confuse the network without interacting with other nodes [6]. The presenceof afailed node prevents ad hoc by "updating wrong route", "responding to outdated routing information", "changing routing updates or advertised incorrect routing information" and "dynamic characteristics" of MANET [7], [8], [19], [10].

The MANET routing mechanism is completely dependent on the coordinating and participating nodes of neighboring nodes. [9] Disobedient behavior can lead to good data loss and network imbalance. A robust, stable, and secure RT-Protocol is needed to attain quality and security performance paradigms to effectively maintain node connectivity and mobility. This effectiveness can provide better security.

The trust system can be used to present available network security services such as "quality assessment", "access control", "authentication", "M-Node detection" and "secure resource sharing" [11], [12], [13], [8], [14] receivedinformation. Therefore,it is important to periodically approximate the trust level of anode depend on definite matrices and computations.

In Section3, it discusses the "Node Trust Predicting Approach (NATR)" identify the node trusts in order to begin further secure communications on MANET. In these networks, numerous approaches associated with trust computinghave been proposed [15], [16], [17], and temporary real-world results have beenobtained. The proposal provides an inclusive node trust forecast method depend on *Success rate of RREQ*, *Success rate of RREP*, and *Data Success rate* node trustto progress MANET security managing node-level trusts.

2 Related Works

By establishing a TM network mechanism to improve network security efficiency [1], [2]. Trust has attracted attention in many areas of applying security systems is becoming more and more important in wireless networks [7], [18]. Each document method has its own qualification and filter issues. Trust-based security technology is importantand hasbeen studied in MANET-based approaches in much recent literature [19], [20], [21]. The rich literature on trust and Network management makes us highly recommend this to Become important and exciting area for research.

There are many changes in trusts and functions, and their concepts lead to differences in TM terms. Although prevention-based methods can prevent misconduct, M-Nodes still have the opportunity to contribute to the routing process and corresponding routing issues. Knowing the wireless security design and multi-level security mechanisms, this is very important for secure communications in the future.

Govindan et al. [5] presented a specified survey of different trusted computing schemes of MANET. It presents a MANET design a variety of perspectives on trust impressions, the attributes that should be deliberate when extending trust metrics, and the ability to compute trust. It recommends a comprehensive assessment of the several trust calculation methods and a comparison of various attack model and calculation requirements. It also analyzes various documents of dynamics trust computation.

Z. Wei et al. [3] proposed a TM system. The trust framework consists of two parts of surveillance: "direct monitoring of trust" and "indirect monitoring of trust". The value of trust, which is monitored directly from the observer node, is monitored using the Bayes assumption, an uncertainty hypothesis and can describe the complete "probability model". On the other hand, DST (Dempster-Shafer Theory) is used to indirectly monitor indirect information about adjacent nodes (also known as controlled nodes) indirectly to derive trust values, and DST is another type of uncertainty conclusion that can be drawn indirectly. By integrating these two components into a trust model, it can obtain an additional enhanced trust value for further monitoring in MANET.

Pirzada et al. [22] proposed a direct trust calculation based on routing guidance. Describes confidence as a fractional value in [0.1] and evaluates the performance of the AODVandDSR protocols and analyzes them using the proposed trust scheme. In this case, the node always monitors neighbors to create and update trust relationships.The treatment of uncertainty of trust as noticeable node was performed correctly, using entropy to develop a trust model and to assess trust values through direct observation. Compared to direct observations in trust assessments, "indirect or indirect information" may be necessary to assess the trust of control points. To illustrate, a set of proofs from adjacent nodes can identify M-Node in good condition for one observer rather than another.

An RT-Protocol based on the "Security Aware Routing (SAR)" mechanism [23] converts the "AODV Routing Protocol" [24] into a trust hierarchy containing integration nodes for path evaluation and classification. The protocol enforces trust levels at the organization level and uses a shared key for every layer so that nodes be able to specify security prerequisites when applying for routing. Only nodes that satisfy that node can support the path. But how to classify "trust node", "key distribution" and other key awareness is an important area of current research work.

Predicting node trust dynamically means that node trust must vary based on its behavior. Non-transitive signifies "if node-A trusts Node-B and Node-B trust Node-C, then Node-A inevitably trusts Node-C". The asymmetrically means, "if Node-A trusts Node-B, Node-B essentially does not trust Node-A". The resources of the trust estimate that depending on the perspective usually come from the behavior of the node. Different stages of the process can be reached through different trust relationships. For example, if the nodeconsumes lessenergy than it cannot self-guarantee the message sent to its neighbors.

In this case, the energy level of the node decreases, but the "security trust factor" determined by the node does not change due to the state. To calculate the level of trust in the node, it is important to understand the various implementation functions used for definitions, measures, and trust calculations.

The trustreliability of the metric node is the reliability and validity of the information that the node's agent receives or transmits in each context. The MANET routingprotocol is used to evaluate SAR's proposed protocol. The followingsection describes the process of transmitting keys and the transmission of confidence calculation and routing methods.

3.Proposed Node Authentication and Trusted Routing Approach

The proposed "Node Authentication Trusted Routing Approach (NATR)" is performs the three-step process to complete the required node trust level. To ensure its security, it obtains a trusted certificate from Certified Authority (CA) consisting of "public key as CA_{pub_key}" and "private key as CA_{pvt_key}" and validates the node during data redistribution based on these keys. In the second step, the node accomplishes the trust level and third step based on individual node trust level, secure route is established and transaction commences.

3.1.Acquisition of Node Authentication

The certificate authority CA helps the nodes to authenticate themselves with the members in the network before they get joined and start a new communication. The secure trust certificate once issued cannot be revoked or expired during the lifetime of the network. If the value of the node falls below the threshold, the certificate expires. This means that the validity of the certificate can continue until the reputation is maintained. In this case, it wants to identify nodes with illegal certificates and do not invade M- nodes during routing. The certificate provided by the CA includes the trusted key which used for authentication, CA_{cert} expressed in Eq.1.

Each node that is supposed to work as a MANET node receives a public/private key pair *(ND_{pub_key}, ND_{pvt_key})* on construction time. The public key ND_{pub_key} is used as the identifier or node-*ID* of node *N: ND_{ID} = ND_{pub_key}*. This identifier can and must be used in any MANET that supports the security. For routing purposes, the node creates a crypto based address from the node-ID by using a hash function: $ND_{CBA} = h(ND_{ID})$. In order to prevent creation of new node-IDs by nodes, we need to introduce a Trusted Third Party (TTP). This TTP is a certification authority (CA) signing the node-*Ids*.

$$CAcert = Enc_{CA_{pvt_{key}}}\left(N_{pub_{key}}\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots Eq.1$$

3.2.Trust Computation

Node trust is estimated by the node's physicalneighborsbased on historical interaction information. The packet transfer rate is used as the only observablefactor in assessingthis reliability. Two confidence factors that control packet and data packet rates to determinethe overallhistorical trust of the evaluated (or monitored) node.

In a mobile network, all packets can be divided into two types: control packets and data packets. The correctness of control packets plays an important role in establishing the correct route in thenetwork. Therefore, the forwarding rate is divided into two parts: the control packet andthe datapacket forwarding rate. It is counted using control and data packet forwarding counters.

The indication of a node trust is calculated in terms of its authentication, data transfer, and data loss using three monitoring aspects of a node activity. The process of effective data packet delivery and control packet is measured based on the confirmed data delivery being received by the DEST-Node or intermediate node.

These monitoring data are used to calculate the node trust calculation value as the "NTP_{value}" of the node.

Each of these values is recorded in each data packet sent by participating intermediate nodes. Data delivered successfully through a node and the request successful delivery packets, and reply successful delivery increases the number of node points by 1. these parameters can be represented as,

SR: is defined as the, R_Req success rate is calculated based on number of neighboring nodes who have successfully received (rreq) from the source node.

SP: is defined as the R_Rep success rate, which is calculated as successful replies (rrep) received by the source node which has sent the rreq.

SD: is the data success rate, calculated based on successful data delivery through a node.

Let's compute the *SR, SP, and SD* using the Eq.2, 3, and 4. as follows

$$SR = \frac{N_{req}}{Pkt_{req}} \ldots\ldots\ldots\ldots\ldots. Eq. 2$$

Where,

*N_{req}*is no.of request packets successfully received (RREQ-Route Request) from a neighboring node.

*Pkt_{req}*is total number of request (RREQ) packets sent by a node.

$$SP = \frac{N_{rep}}{Pkt_{rep}} \ldots\ldots\ldots\ldots\ldots. Eq. 3$$

Where,

*N_{rep}*is no.of request packets successfully received (R_REP-Route Reply) from a neighboring node.

*Pkt_{rep}*is total number of request (R_REP) packets sent by a node.

$$SD = \frac{N_{ds}}{d} \ldots\ldots\ldots\ldots\ldots. Eq. 4$$

Where,

*N_{req}*is no. of data packets delivered successfully through a node.

d is total no. of data packets sent.

Based on these three "SR*", "SP"and "SD" rate*values, it uses the Eq.5 to calculate the Trust level of a node. It is used by the execution time trusted node to route data from the SRC-Node to the DEST-Node.

$$T_{Level} = P_t\big((R\_REQ) * SR + (R\_REP)SP + (DATA) * SD\big) \ldots\ldots\ldots.. Eq. 5$$

Where,

T_{Level} is Node Trust level, P_t time factorial of R_REQ, R_REP, and DATA sent respectively

SR: is R_REQ success rate, SP is R_REP success rate, and SD is data success rate

The value of *NT_{level}* is used as value constraints for the node to consider communication and is utilized as the SRC-Node. In the subsequent section, it will discuss the trust prediction routing method utilizing the *NT_{leuel}*.

3.3.Route Acquisition

The primary goal of the routing method in MANET is to present proficient data routing. Every node in the proposed protocol transmits data via the discovered path and predicts the *NT_{leuel}* of each node by monitoring the three activities mentioned. The proposed NATR protocol presupposes that the nodes in a MANET are reliable and trustworthy. Using Eq.5 trust value of a node is computed.

The SRC-Node sends the packet to the DEST-Node using the cached route from the route manager. Primarily, all nodes *NT_{level}* are believed to be 100%. To begin with, SRC-Node chooses the shortest hop path. During routing, every node requires its neighbor nodes to generate a *CA_{cert}* certificate to obtain authentication before broadcasting the packet. If data is successfully transmitted it update SR, SP, and SD success is updated based on these values

"NT_{level}" is calculated and updated in the routing table. The procedure of node selection and routing is presented in Algorithm1. A description of the node trust routing table for a given scenario in Figure.2. is given in Table1.

Algorithm 1: Data Routing based on the Node Trust level(Input: Network, Output: Node Trust value)

```
Data Transmission by Source Node, S
Sadd: Source address
Dadd: Destination address
TransmitData (Sadd, Dadd, Data, seq_no);
FH: First Hop nodes
NTL: Node Trust level value
Begin
Procedure: TransmitData (Sadd, Dadd, Data, seq_no)
Input: Node Trust level
Output: Successful data routing
// Threshold of NTlevel Node Trust level Value
Th_NTP = 60%;
// Read First Hop Nodes from Routing Table
FH_N[x] = getFirstHop_Nodes();
P = Number of data packets to transmit.
H =sizeof (FH_N[x]);
For (d=0, d<P, n++) Loop
        For (h=0, h<H, h++) Loop
            FH=FH_N[x h];
            NTlevel=getNodeAuthentic_Rate(FH)
            If NTlevel>=Th_NT then
             TrData(Sadd, Dadd, Data, seq_no) // Transmit Data
            Else
                Check for Next available Hop NTlevel;
            End If
        End For
    End For
End Procedure
```

For instance, in Table 1, it illustrates five routes to the destination, and the first-hop and "NT_{leuel}" for each route. According to the route discovery, the most efficient and shortest route is R1, but according to the "NT_{leuel}", the first hop of the route R2 is more reliable than the route R1. Therefore, routing of data through R2 instead of R1 is feasible.

Table 1: Source Node Routing Table

Sl.No	Route	Prev_Hop	First_hop	NT_{Level}
R1	6,3,4,2,D	S	6	41
R2	4,5,3,8,10,D	S	4	70
R3	6,3,8,5,12,D	S	6	58

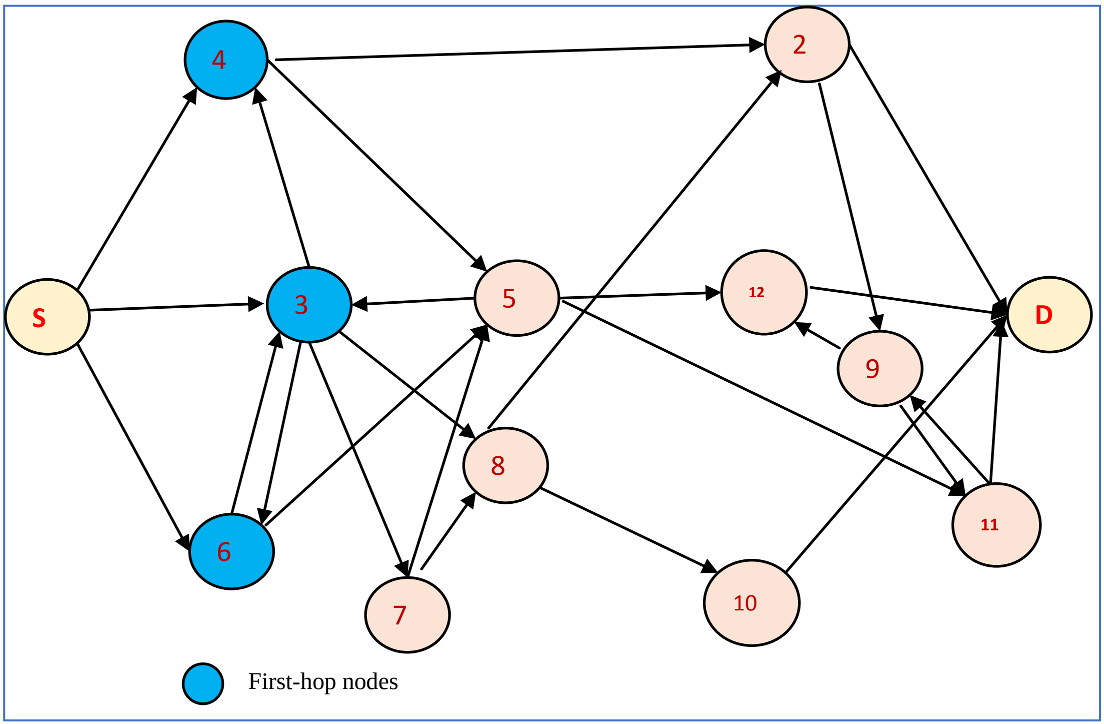


Figure1: An Example for a Node Authentication and Trust Routing Approach

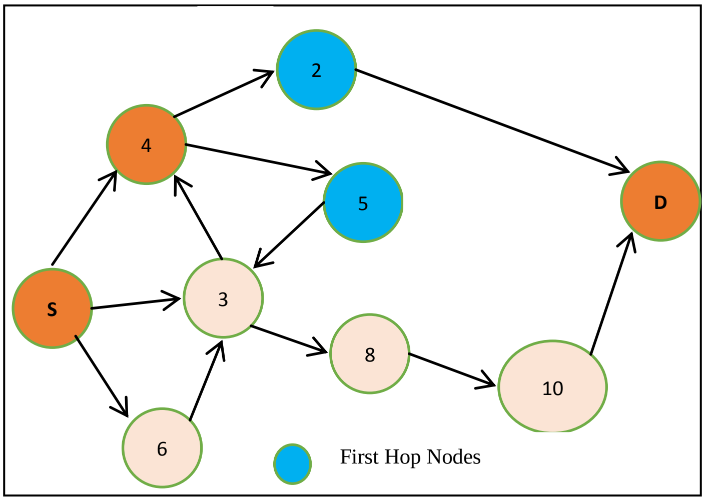
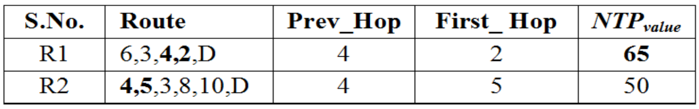


Figure.2: Route discovery

The "intermediate node" also follows the same arrangement as the "original SRC-Node" function. Table 2 and Figure 2. illustrates the node routing table for Node 4, which has two hopes. According to this table input and its first_hop "NT_{leuel}", chooses the route node R1 because its "NT_{leuel}" is superior to the R2 node.

Table 2: Routing Table for Node-4 as Intermediate Node



S.No.	**Route**	**Prev_Hop**	**First_ Hop**	NTP_{value}
R1	6,3,**4,2**,D	4	2	**65**
R2	**4,5**,3,8,10,D	4	5	50

The SRC-Node executes the "sequence number of the packets" list sent by it. After the successful acknowledgment is reached, the source will update the SR, SP, and SD of every node in the route. This dynamic routing depends on runtime "NT_{leuel}" provides reliable and secure routing and ensures the delivery of acknowledgments in the case of arbitrarily selected nodes or predefined routing nodes. The entire process of NATR is described as:

In figure 2. Node S is the source node and the destination node D. If source node S has to share the data with a destination node, using the cached route from the route manager. During routing, every node requires its neighbor node to generate a CA_{cert} certificate to obtain authentication before broadcasting the packet. If it is successful it will update the node validity and similarly, update data successful transmit or loss of data will be updated. These values are continuously observed and calculate SR, SP, and SDvalues and at last NT value is calculated. In order to obtain an accurate node’s trust value, our model distinguishes the different influence of our model distinguishes the different influence of each interaction interval. Using the time stamp mechanism to analyze each interaction interval (e.g., set interval $\Delta t = 30$ (s)). Till to current time t, there are n intervals from time 0 (i.e., [t1, t2, ..., tn]). Trust values are updated in the routing table shown in Table 1.

Here source node S illustrate the five routes to the destination and the first hop NT value for each route. The first hop nodes of S are 3,4,6 and their NT values are 35, 68, 60 and 38 respectively computed by using Eq.5. S nodes routing cache after triggering an update shown Table 2. According to route discovery process R1 is efficient and shortest route. But according to NT_{Level} value route R2 is more reliable than the route R1 and R4. Therefore, routing of data through R2, node S routing cache after triggering update as shown in Table 3.

Table 3: Node S Routing Cache after triggering an update

S. No	**Routing Cache**	**First Hop Node**	**NTP_{value}**
R1	(S,6,3,4,2, D)	6	38
R2	(S,4,5,3,8,10, D)	4	68
R3	(S,6,3,8,5,12, D)	6	60

Similarly, intermediate node 4 (route R2 first hop node) follows the same procedure as the source node S until D is identified. The node 4 illustrate two routes to the destination R1 and R2. Node B’s Routing Cache after triggering an update is shown in figure 4.3 and routing table is shown in Table 4.4. the first hop nodes of 4 are 2, 5 and their NTP value is 65 and 50 respectively computed by using Eq.3.

Table 4: Node 4 Routing Cache after triggering an update

Node	**Routing Cache**	**First Hop Node**	**NTP$_{value}$**
4	(4,2, D)	2	65
4	(4, 5,3,8,10, D)	5	50

Node 5 is having less trust value. The remaining node 2 has highest NT value. Node 2 transmits the packets to destination D receives packets through (S,4,5,3,8,10, D), (S, 4, 2, D). routes which carries the trust values as 68, 65 respectively. Hence, node S selects the route (S, 4, 2, D), as it has high trust value.

4. EMPIRICAL ASSESSMENT

It adopted the “AODV protocol” to estimate the “NATR protocol” and have evaluated the helpfulness of our planned protocol and compared them with “SAR” [20] and “AODV”. As it adds security factors, the size of the route request and routing packet headers will increase. The proposed NATR executed on the same.

We execute the experimentation based on the Table-5 simulation factor for a time of "600 seconds" with an RWP movement behavior model with varying speeds between "0 to 100 m/s". We execute the simulation in six dissimilar speed as configured in Table-5. For data routing, we used "15 source-target pairs" of "constant bitrate (CBR)" traffic of "4 packets per second", and each "512 bytes" in size. The assessment was conducted in two different situations. First, there were not any misbehaving nodes in the network, followed by 25% of the misbehaving nodes added. The experimental outcomes demonstrate the "overhead introduced" caused by security enhancements and "throughput", comparisons.

Table 5: Simulation Parameters

Configuration	**Parameter Values**
Simulation Dimension	"1000m X 1000m"
Distributed Nodes	"50"
RWP Mobility	"0 to 20 m/s"
Source-Target Pairs	"15"
Size of Pkts in Bytes	"512"
Rates of Pkts Transmission	"4 pkts/sec"
Variation of Mobility (m/s)	"0,20,40,60,80,100"

The assessment was conducted in two different situations. Primary, there are no nodes with abnormal behavior in the network, followed by nodes with 25% behavioral anomalies. The experimental results display the overhead caused by security enhancement and throughput comparison.

All nodes are up and running during route discovery. However, the nodes that randomly identify 25% of the behavioral anomalies in the track simulator will behave abnormally, ignoring all packets and generating incorrect confidence predictions. However, the use of signature verification in NATR can detect any type of packet modification attack,and dropping the packet can isolate the abnormal node from the network. To evaluate performance, we identified the following “packet delivery ratio”, “control overhead", “end to end delay”, and " throughput" metrics. The results analysis as follows:

4.1. Results

A. Throughput:

Figure4.5 show the throughput. The nodes' mobility varied from 0 to 100 m/sec; the corresponding throughput was observed in the absence of malicious nodes and the presence of malicious nodes. In the presence of 25% malicious nodes, all methods perform the same throughput. For node mobility 20m/sec the throughput for NATR is 0.958, SAR is 0.870 and TMS is 0.902. NATR obtains 28% to 35% higher throughput than TMS. When node mobility is varied from 40 to 60m/sec, AODV and SAR illustrate lower throughput than NATR. Compared to SAR and AODV, NATR to get a better throughput of up to 25%, because of secure data routing by trusted nodes. The NATR achieved improved throughput than the existing methods for MANET.

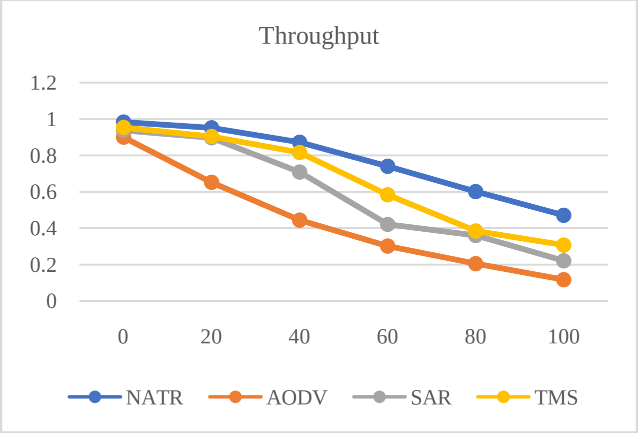


Figure. 3: Throughput (" Presence of Malicious nodes")

B. Control Overhead:

Figure4.7 shows routing overhead. The corresponding routing overhead was observed in the presence of malicious nodes with varied node mobility, that NATR shows the best performance compare with SAR. AODV illustrates the high overhead than NATR. It can be observed that when node mobility increased, the NATR produces the lower overhead compared to SAR, and AODV has the highest overhead. Improvisation is based on past performance to determine honest nodes, rather than punishing all nodes in the route as its traditional methods helping to keep the network layer and improve performance.

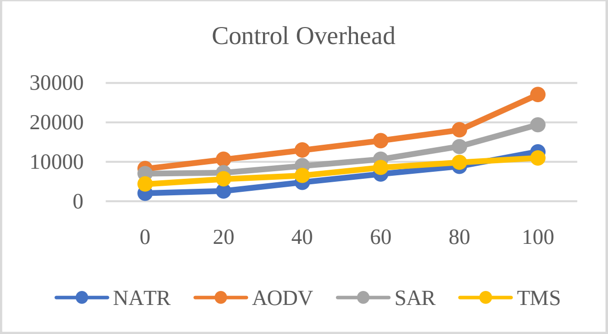


Figure.4.: Control Overhead

C. Packet Delivery Ratio

The packet delivery ratio, results are shown in Figure 4.9. The proposed NATR is compared with TMS, AODV, and SAR. The nodes' mobility varied from 0 to 100 m/sec; the corresponding packet delivery was observed in the presence of malicious nodes. In the presence of 25% malicious nodes, all methods perform the same packet delivery. For node mobility 20m/sec the throughput for NATR is 0.95, SAR is 0.870 and TMS is 0.952. NATR obtains 24% to 30% higher throughput than TMS. When node mobility is varied from 40 to 60m/sec, AODV and EAACK illustrate lower throughput than NATR. Compared to EAACK and AODV, NATR to get a better throughput of up to 25%, because of secure data routing by trusted nodes. The NATR achieved improved throughput than the existing methods for MANET.

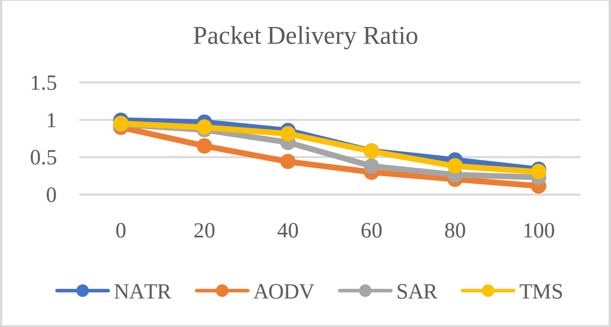


Figure.5.: Packet Delivery Ratio

D. End to End delay

It measures the average time taken by a node for data packet delivery, in the presence of malicious nodes are shown in 4.11 demonstrates the "end-to-end delay" assessment of the proposed NATR is compared with SAR, AODV and TMS approaches. The packet delivery is reduced due to the node's mobility increased in the presence of malicious nodes. For node mobility 20 m/sec, all methods show a nearby delay up to 10 msec. When node mobility increases from 40 to 60m/sec SAR and TMS shows increases, and NATR shows less end to end delay. In the presence of malicious nodes, NATR shows a nearby end to end delay up to 8 msec, compared to SAR. The NATR provides secure data routing by trusted nodes. NATR to get 10% less end to end delay compared with SAR.

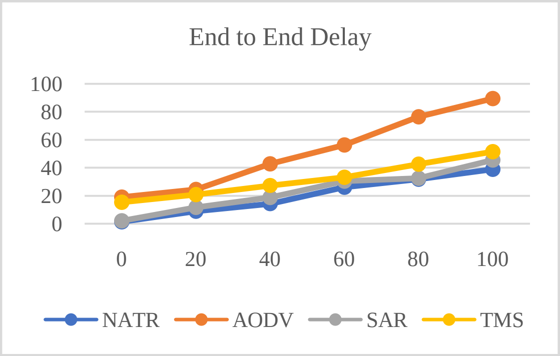


Figure.6. End to End delay (“Presence of Malicious nodes”)

Conclusion

We propose an innovative "Trusted routing protocol", NATR for MANET. NATR authenticates the routing node based on the "node authentication" and "trust level" computed during communication. NATR manages multiple routes to reach the destination node. Every node in the network accumulates the "local trust values" of all other nodes and maintains a routing table. NATR computes a trust value for all hosts on the first hop. Intermediate nodes, route, and data packets choose the route with a higher value for trusted nodes. NATR-based security hardening mechanisms help improve PDR throughput during communication. Empirical results show 25% higher PDR with minimal overhead and delay. This increase can lead to a decrease in the confidence value and convergence time.

References

[1]. Z. Movahedi, Z. Hosseini, F. Bayan, G. Pujolle, "Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey", International Journal of IEEE Communications Surveys & Tutorials, Vol. 18(2), Pp. 1287 - 1309, 2016.

[2]. K. Ullah, R. Das, P. Das, A. Roy, "Trusted and secured routing in MANET: An improved approach", IEEE International Journal of Symposium on Advanced Computing and Communication, Pp. 297 - 302, 2015.

[3]. Z. Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning", IEEE Transactions On Vehicular Technology, Vol. 63, No. 9, November 2014.

[4]. Ullah, R. Das, P. Das, A. Roy, "Trusted and secured routing in MANET: An improved approach", International Journal of IEEE Symposium on Advanced Com. and Comm., Pp. 297 - 302, 2015.

[5]. K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, 2012.

[6]. L. Buttyan and J.-P. Hubaux, "Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks", EPFL-DI-ICA, Tech. Rep. DSC/2001/001, Jan. 2001.

[7]. J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks", IEEE Communications Surv. Tuts., Vol. 13, no. 4, pp. 562-583, 2011.

[8]. A. Ahmed, K. A. Bakar, M. Ibrahim Channa, K. Haseeb, A. W. Khan", A Survey on Trust-Based Detection and Isolation of Malicious Nodes In Ad-Hoc and Sensor Networks", International Journal of Frontiers of Computer Science, Vol. 9(2), pp. 280-296, 2015.

[9]. R. Changiz, H. Halabian, F. R. Yu, I. Lambadaris, and H. Tang, "Trust establishment in cooperative wireless relaying networks", Wireless Communications Mobile Computer, Sep. 2012.

[10]. Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", In ACM/IEEE Int. Conf. on Mobile Computing and Networking (MOBICOM'2000), Feb. 2000.

[11]. M. S. Pathan, N. Zhu, J. He, Z. A. Zardari, M. Q. Memon, and M. I. Hussain, "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs", Future Internet, 10(16), DOI:10.3390/fi10020016, 2018.

[12]. N. Marchang, R. Datta, S. K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks", International Journal of IEEE Transactions on VehicularTechnology, Vol. 66(2), Pp. 1684 - 1695, 2017.

[13]. T. Shu and M. Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", International Journal of IEEE Transactions On Mobile Computing, Vol. 14, No. 4, Apr. 2015.

[14]. L. Kagal, T. Finin, and A. Joshi, "Trust-based security in pervasive computing environments", IEEE Computer, Vol. 34, pp. 154-157, 2001.

[15]. Sarvanko, M. Hyhty, M. Katz and F. Fitzek, "Distributed resources in wireless networks: Discovery and cooperative uses", In 4th ERCIM eMobility Workshop in conjunction, 2010.

[16]. M. A. Ayachi, C. Bidan, T. Abbes and A. Bouhoula, "Misbehavior detection using implicit trust relations in the AODV routing protocol", In International Symposium on Trusted Computing and Communications, Trustcom, pp. 802-808, 2009.

[17]. A. Boukerch, L. Xu and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks", In Computer Communications, no. 30, pp. 2413-2427, 2007.

[18]. J. Hassan, H. Sirisena, and B. Landfeldt, "Trust-based fast authentication for multi-owner wireless networks", IEEE Trans. Mobile Computer, Vol. 7, no. 2, pp. 247-261, 2008.

[19]. S. Bu, F. R. Yu, P. Liu, P. Manson, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks", IEEE Trans. Veh. Technol., Vol. 60, no. 3, pp. 1025-1036, Mar. 2011.

[20]. S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks", in Proc. 2nd Workshop Economy. Peer-to-Peer System, pp. 1-6, 2004.

[21]. Wang, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length", International Journal of Network Computer Application, Vol.34, No.4, pp. 1138-1149, 2011.

[22]. A. Pirzada and C. McDonald, "Trust establishment in pure ad-hoc networks", Wireless Personal Communications, Vol. 37(1-2), pp. 139- 168, 2006.

[23]. S. Yi, P. Naldurg, and R. Kravets. Security-aware ad-hoc routing for wireless networks. In MobiHOC Poster Session, 2001.

[24]. C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", IETF RFC 3561, Jul. 2003.