International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.6982
***Article Received**: 02 April 2023 **Revised**: 15 May 2023 **Accepted**: 29 May 2023*

Secure Routing Protocols Comparison Analysis Between RNBR, SAA, A-UPK

Dr. T. Shekar Reddy[1], Dr. T. Shyam Prasad[2], Dr.Y. Rama Devi[3]
[1]Telangana Mahila Viswavidyalayam
Department of CS,University College For Women(A)
Hyderabad,India
shekarreddy08@gmail.com
[2]Anurag University
Department.Of CSE
Hyderabad,India
shyam.tprasad@gmail.com,
[3]Osmania University
Department Of CS, CBIT,
Hyderabad,India
yrd@cbit.ac.in

Abstract The advent of wireless communications and the development of mobile devices have made great strides in the development of roaming communications. The MANET mobile network was developed with the ability for mobile devices to quickly self-configure and extend wireless coverage without infrastructure support. Security is one of the most important areas of research and plays a vital role in determining the success of personal and commercial telephone systems.Therefore, this study focuses on systematically examining MANET security and accountability issues and analyzing the performance of solutions proposed by three different design approaches to security systems.First, it provides an approach for identifying trusted nodes employing the proposed RNBR method for secure routing.it provides a Self-Assured Assessment (SAA) method to estimate node stability. Its main goal is to contribute to a self-assessment-based reliability assessment mechanism that provides a reliable and reliable pathway.it provides a new authentication method to prevent forgery attacks. It supports authentication mechanisms to prevent RF attacks and ensure secure routing development.The main Objective of this paper is compare to packet delivery Ratio ,Control Overhead, Packet Drop Ratio in different secure RNBR,SAA,A-UPK Routing Protocols in MANETS.

Keywords: RNBR, SAA, UPAK, MANET, Routing, MAL_NODES.

I. INTRODUCTION

1.1 MOBILE AD-HOC NETWORK

The emergence of wireless communications and the proliferation of mobile devices have significantly enhanced the development of lively communications. On wireless infrastructure, self-initiated and portable wireless broadband connections can lead to the development of MANET. Mobile devices on these networks are often called nodes. Its work is mainly involved in emergencies, such as natural disasters, emergency response plans, and so on.

MANET has been extensively utilized in various military and civilian projects because of its wide and powerful environment. It communicates in a multi-hop manner over a wireless ad hoc network. Mobile node users work together to build a network without major infrastructure support such as access points or base access points. As revealed in Figure 1.1, there are essential features such as topological conditions, inadequate bandwidth, and restricted sources when MANET configurations are developed. The key point is to optimize resource usage, and secure deployment is a major challenge for MANET.

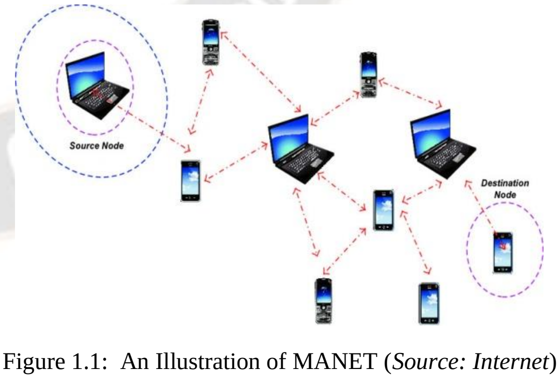


Figure 1.1: An Illustration of MANET (*Source: Internet*)

MANET is said to be available when the nodesare ready to send a message and the other nodesare ready to receive it. These mobile nodes operate as hosts and routers. This allows packets to be sent to other mobile nodes in the network via the bandwidth of the mobile SRC_NODE. All nodes in the network operate as an active task in allowing the ad-hoc root protocol to deploy multi-hop routes to other nodes in the network.

MANET devices have limited resources to limit access range, such as bandwidth, storage space, and battery [1]. Therefore, traffic must be efficiently distributed among mobile nodes. The MANET routing protocol must accurately distribute routing among mobile nodes. MANETs consist of mobile devices equipped with wireless communication equipment. MANET's main features are rapid deployment, self-configuration, and multi-hop wireless connectivity without a central location. Link failures are common due to portability and resource constraints. The issues of the MANET transport protocol and the overall environmental change have been discussed comprehensively and coherently [2].Nodes in a particular network have restricted transmission space and limited processing, storage, and energy resources. These limited resources on a given wireless network are a significant challenge for integrating security measures to manage security and privacy. Therefore, MANET's security and privacy policies are very difficult and complex research requirements.

II. SECURITY CHALLENGES IN MANET

As MANETs function differently from standard wired and wireless networks, they must address new challenges related to security and privacy concerns. Because MANETs cannot handle centralized management or synchronization, network providers and their counterparts are changing rapidly, and because networks are designed to collaborate, achieving these goals is much more difficult than traditional networks.

Security and privacy are considered fundamental issues, mainly due to other node activity and trust. It can classify their behavior into two main groups, and this arbitrary behavior of nodes causes problems.

- **Selfish Activities*:*** Resources are very limited on most portable mobile devices. So, instead of using local resources to send packets, nodes must send their traffic using the MANET. These external packets can prevent themselves in the following ways,
  - ✓ It does not simply forward packets received at the intersection to other nodes.
  - ✓ Defend the options of these choices along the way. Ability to reject redirect request redirects or change turn-by-turn responses and behave by including nodes too long and offensively.
- **Malicious Activities*:*** For a variety of reasons, MANETs may have a point where they are actively attacking the network through anomalous activity. Because every node is part of the basic navigation structure, such an attack can be easily carried out and can do a large number of damages. It undergoes various kinds of attacks such as,
  - ✓ Denial of Service*:* An attacker can disrupt the flow of information at the wireless level or through a network or path structure. It can create problems by creating "routing loops", "black holes", etc.
  - ✓ Route Fabrication*:* Attackers can attack online messages and influence their path to facilitate universal access to packets and redirect packets through unambiguous nodes.

After the above activity, some nodes reveal sensitive messages that attackers are trying to access. This opens up data security and privacy. All of these public issues motivate it to contribute to the security, privacy, and applications of future mobile networks. Its primary purpose is to address every feature of mobile device protection, functioning, assessment, operation, and administration through security methods, protocols, and designs.

III. RELATED WORKS

The main purpose of this study is to provide a solution to the MANET security problem using reliable computing methods. Trust is an essential characteristic of a MANET. It allows the organization to deal with the insecurity and uncontrollability reason by the liberated will of others.

This presents a novel protocol based on node trust calculation and node behavior prediction for effective TM and quality of service for three purposes:

- **Identification of Reliable Nodes for secure Routing**

It is always difficult to protect nodes from internal and external attacks that affect reliability. This task contributes to a trust-based routing protocol by identifying the most reliable nodes in the network for secure routing and high throughput. The goal is to maintain several reliable routes to the destination for effective communication.

- **Node Trust Estimation through Self-assurance Assessment**

The improved version of MANET provides excellent support, which is well suited for urgent purposes. However, at the same time, due to its low energy and computing power, it suffers from the risks and difficulties of providing high security and reliability due to its dynamic behavior and full reliance on anonymous nodes for communication cycles. Literature studies have shown that the use of confidence estimation is low overhead and expenses. It aims to contribute to a self-assessment-based

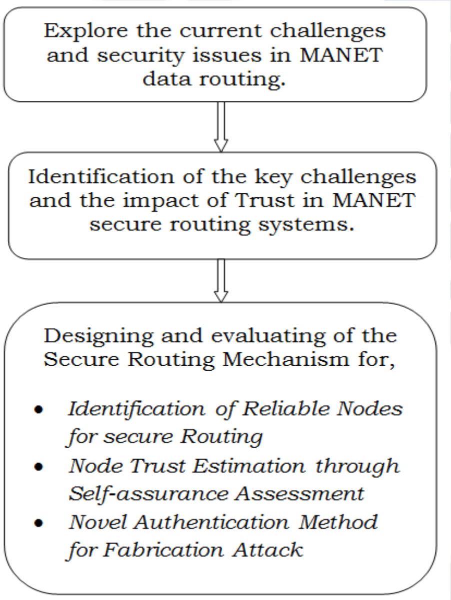
International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.6982
***Article Received**: 02 April 2023 **Revised**: 15 May 2023 **Accepted**: 29 May 2023*

trust estimation mechanism that ensures reliable and secure routing.

- **Novel Authentication Method for Fabrication Attack**

Route fabrication (RF) is a type of attack that invades networks by propagating information and generating fake IDs. After giving the impression of normal behavior, it is very difficult to identify falsehoods in a node's hypothetical behavior. In addition, in the event of an RFA attack, many packets of communication will be generated if the directional information is changed during traversalor data processing. It aims to contribute to authentication mechanisms that prevent RF attacks and strengthen secure routing.

The goal of this study is to build a solution with the above goals to improve MANET security and quality of service by leveraging trust and node behavior prediction and computation through a methodological process as shown in Figure 1.2



1.Identification of Reliable Nodes for secure Routing: It first discuss node reliability and show the mechanisms for developing reliable node-based routing approaches for reliable and secure routing.

2. Node Trust Estimation through Self-assurance Assessment: It Describe and present the design of a self-assurance approach for evaluating confidence calculations and assessments.

3. Novel Authentication Method for Fabrication Attack: It first discusses path making (RF) attacks and path protection approaches, and later show A-UPK mechanisms to prevent RF attacks.

IV. EXPERIMENT EVALUATION

4.1 Reliable Routing

To carry out the reliable routing, every node in this network must evaluate the reliability of the other nodes. The trust values are usually calculated based on previous observations made by it. Each time a node *V* transmits information via the route, it is considered trusted, and otherwise, it is judge as corrupted. In such cases, *V* will review the new route for transmitting the information. In this work, DEST_NODE *D* transmits an explicit acknowledgment to guarantee the reliability of route *R*.

We know that a limited count of routes as *G* gets to the DEST_NODE *D*. The SRC_NODE *S* determines a trusted path relies on the trust value of every node. *S* evaluated the confidence value of every route by supervising the packets transmitted through the route acknowledgment of every packet. It calculates the trustworthiness *T* to determine reliability. It is based on two elements A_v and B_v for a node *V*. The A_v symbolized the quantity of successful deliveries and B_v represents the number of failed deliveries. The reliability of node *V* is computed utilizing Eq. (4.1),

$$T_v = \left(\frac{A_v}{A_v + \beta B_v} \right) \tag{4.1}$$

Let's considered for a Node *S* transmitted 25 data packets, where a IMED_NODE *v* perform the following transmission.

No. of successful delivery, $\boldsymbol{A_v = 17}$,

No. of delivery fails, $\boldsymbol{B_v = 8}$,

and If the punishment Rate$\boldsymbol{\beta = 3}$,

then the based on the Eq. (4.1) the computed Trustworthy , T_v of this node will be,

$\boldsymbol{T_v = 17/\,(17+(3*8)) = 0.41}$

The reliability of the path from {*S*, V_1, V_2, ..., *D* } is able to be easily described as a growth of the reliability of every one node on that route. On the lengthy route, reliability is able to be unreasonable. After the path has opted, *S* adds the series number *Q* and the opted route for sending information packet by signs it via that route.

Each IMED_NODE needs to resend such a packet, rather than validating *S's* signature with *P* probability. When the node *D* gets a packet via the route as $R = \{S, V_1, V_2 \ldots ,D\}$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.6982
***Article Received**: 02 April 2023 **Revised**: 15 May 2023 **Accepted**: 29 May 2023*

withthe signed acknowledgment $M = \{ACK, V_{id\_n}, \ldots, V_{id\_1}, Q_s\}$ through same path. An IMED_NODE that validates *D's* signature with *P* probability and resends this information reverse to *S*. The *S* preserves it in a table of serial numbers of packets transmitted and the previously utilized routes along with the timestamps of an acknowledgment as a t_{ack}.

It updates the data entry for every node in the route that gets the acknowledgment. If no acknowledgment is received before the tack expires, it punishes the complete node in the path with growing in delivery failures. The *B* value reduces reliability and reliability during calculation. The IMED_NODE V_n sends a signed path fault information to *S* as $M=\{REER, V_{id\_n}, \ldots, V_{id\_1}, Q_s\}$, if it cannot correspond with the subsequent hop because of a link fault while sending a packet all along in a particular path.

So, in a path if we have 5 node from SRC_NODE to DEST_NODE, then the reliability of the entire path is being computed on each iteration of data transmission is illustrated in Table 4.1.

Table 4.1: Illustration of Reliability computation

No. of Pkt. Transmitted	No. of Pkt. Delivered	No. of Delivery Failed	T_v Value	Route Reliability threshold >=0.25
10	8	2	0.571	Reliable
10	9	1	0.750	Reliable
10	7	3	0.438	Reliable
10	5	5	0.250	Reliable
10	4	6	0.182	Non Reliable

So, if the reliability go below threshold limit then the path is discarded.

4.2RNBR Simulation Setup

- The proposed RNBR protocol evaluated using a Glomosim Simulator. The RNBR derives the AODV routing methodologies with enhancement of the security mechanism. The required security module is added to the header of the packets to perform the route discovery and data routing respectively.
- The simulation was carried out in a RWP mobility model, where each node change their position as per configured pause time 30 sec and mobility speed between 0 to 25m/sec. The nodes change their position arbitrarily in any direction accordingly the configured mobility speed. It will continue till the end of the simulation time configured.
- A set of 20 source-destination pairs are configured to transmit data during this simulation. Each node transmit data packet at a CBR flow of 4pkt/sec, having a size of 512 bytes. The configured parameter's and its value are presented in Table-1 below.

Table4.2. Simulation Parameters

Parameters	Values
Simulation Time	1000sec
Simulation area	1500mx1500m
No .of nodes	100
Mobility speed	0 to 20 m/s
mobility	Rwp
CBR Rate	4pkts/sec
Pause time	30 sec
Packet size	512 bytes
Malicious nodes	10,20,30,40,50
No. of route maintained	4
Punishment Rate(β)	3
Minimum A trust	0.6

4.3 Self-Assurance Based on the Trust Computation

The MANET functionality of the actual instance has been erroneously changed in some instances for a variety of reasons. This makes the N-Behavior always random in the real instant network. This can also result in the attacks and resources required to preserve network strikes and packet transmitting. It evaluates the behavior of diverse groups for the changes made to the following observations.

- Due to energy loss and misinformation, they can affect nodes and affect potential failures and other malicious attacks, or the self-esteem that protects their sources.
- Appropriate reconstruction that is able to re-establish the trustworthiness of "selfish" or "harmful nodes". This re-establishment might retain to reduce the loss of nodes in the network and also manage the reduction in resource usages.
- A MAL-node is classified as a defective node if its activities go erroneous, and it is not widely believed to be reliable or self-sustaining.
- If the failed node routing operation is constant at regular intervals, the node will be believed again.

There is no particular reason to perform the transformation at the top of the estimate, but this makes the observed changes in the most extensive network scene more common. To simplify this hypothesis and measure accurate expectations, we use probability assessment [85] to obtain a mathematical model. Consider the concept of a network area containing *N* nodes with different categories as *S* for the above node. *S = {"AC", "NA"}*. Especially at time intervals,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.6982
***Article Received**: 02 April 2023 **Revised**: 15 May 2023 **Accepted**: 29 May 2023*

T these nodes can change the behavior of S at the same time. This is expressed as:

$$S = \int_{n=0}^{N} T(Prob\,['AC', 'NA']) \quad (4.3.1)$$

These behavior modification possibilities can be evaluated as E_n and C_n in the process of the instance, where $C_n \in S$,can be given as.

$$E_n = prob\,((E_{n+1} \rightarrow C_{n+1}) \mid (E_n \rightarrow C_n)) \quad (4.3.2)$$

Estimate based on the formula. (4.3.2) in the case of probability estimation [85] in the region S of all nodes N as E_n , here "$n = (0,1,2, ..., n)$". The random behavior of a node, on the other hand, translates into a complete set of confirmation.

Finally, the node operating node t (n) of the current node classifies the future of the category. For example, "C_n is the present condition of the node", and after a while, the behavior transforms from "$C_n = C_n + 1$", and the probability estimate determines that it correlates as follows.

$$M_{a,b}\,(C) = Prob\,(\,P_{n+1} = b,\, C_n \leq c \mid P_n = a) = p_{ab}\,T_{ab}(c) \quad (4.3.3)$$

here, "$p_{ab} = lim_{s\rightarrow\infty}$" and "$M_{a,b}\,(C) = Prob\,(\,P_{n+1} = b \mid P_n = a)$", defines the transformation of the state changes probability among the nodes "a"and "b". It is represented as $T_{jkab}(c) = Prob\,(P_n \leq c \mid P_{n+1} = b,\, P_n = a)$, which communicates to a period among the two kinds of changes between the nodes "a" and "b".

Based on various classifications it makes node changes using the stochastic matrix shown in Table 4.3.1.

Table-4.3.1: Representation of the matrix of Conducts Assurance

	AC	*NA*
Non-Malicious	**1**	0
Malicious	0	**1**

Using this behavior guarantee Table 4.3.1 matrix, the probability of behavior change could be estimated by the node's behavior for the current time "$T_{ab}\,(t) = 1 \mid 0$"in the distribution.

When delivering behavior and the latest behavior, and when changes are measured at a given moment, the node does not change. The outlook for change is measured as zero. The futuristic definition model of a node is self-efficacy based on these estimates. This evaluation model is used to evaluate evaluations and establish secure and reliable communication.

Calculating the reliability of individual nodes typically preserves individual operations such as sending data and processing requests [42]. Reliability or collective guarantee trust (CAT) can be trusted from the A_{Trust} next to the person doing it. Trusting the behavior of related entities describes compiling trusts to see if adjacent nodes are harmful.

Cumulative trust is determined by trust in personal conduct. There are many traditions for calculating cumulative guaranteed trusts [46], [86], which suggest the collective trust of node i as "CAT_i". The Node trust is computed utilizing the individual Total Assured Trust (TAT) through the node over time.

Each node has a maximum of one set trust value. Between "0" and "1", the reliable series of A_{Trust} and CAT combined is among "0" and "1", which is the best CAT for the node that is able to estimate using Eq. (4.3.4).

$$CAT_i = TAT_i \times A_{Trust}(i) \quad (4.3.4)$$

If the node trust as t_{rust} is low, the scheme reduces the collective properties and the threshold drops to the bottom. Therefore, the impact of A_{Trust} affects the cumulative trust that holds certain credentials. All actions used by the node are calculated after changing the action using Eq. (4.3.4), it can find jobs that rely on N-Behavior research and behavioral improvements for opportunities to reestablish trust.

For example,

Let's assume each time period T, has Q interval.

Here, we consider ***1 T = 5* interval**.

and, initial **TAT value** of each node = **1**

and, A_{trust} is computed as,

$$A_{trust} = \frac{\text{Total Count of AC state in a Period}}{\text{Total number of Intervals}}$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.6982
***Article Received**: 02 April 2023 **Revised**: 15 May 2023 **Accepted**: 29 May 2023*

Table 4.2: An illustartion of SAA based Trust computation

Time Period (T)	No. of AC state	A_{trust}	TAT	CAT
T1	3	0.6	1	0.6
T2	4	0.8	0.6	0.48
T3	2	0.4	0.8	0.32
T4	3	0.6	0.4	0.24
T5	4	0.8	0.6	0.48

Here, the higher the CAT the higher the Trust and lower the value lower the Trust. So, according the CAT values SAA decides which nodes to be considered for the communication.

4.4SAA Simulation Setup

Simulation analysis was carried out utilizing the GlomoSim network simulator. It shows the standardized allocation of nodes and additional realistic progression patterns.

Table-4.4: Simulation Parameters

Configuration	Parameter Values
Simulation Time	1000s
Simulation Area	1500m X 1500m
No. of Nodes	100
Mobility	RWP
Mobility Speed	0 to 20 m/s
Pause Time	30s
Packet Size	512 bytes
CBR Rate	4pkts/s
Minimum A_{Trust}	0.6
Malicious Nodes	10, 20, 30, 40, 50

4.5 PROPOSED A-UPK MECHANISM

This segment describes an authentication mechanism that utilizes a UPK to compensate for packet loss in traditional local supervising methods caused by RF attacks. The procedure of the A-UPK method is to reduce the performance of RF attacks, packet drops, and improvisational routing.

4.5.1 Method for Preventing RF Attack and Packet Loss

It uses UPK to design the authentication process to provide a proactive method. MAL-Nodes typically modify the route from the original node and retransmit it to the incorrect destination in an RF attack. This causes the packets to stay on the net for a longer period and escape the network or expire. Therefore, SRC_NODE should be replicated over the network and re-sent the abandoned packet using more bandwidth.

In an RF attack, a MAL-Node forwards the packet to the wrong phase, causing the packet to be lost. In BLM [93], the DEST_NODE path acceptor node is affected by the attacker and abandons the packets, or creates another inaccessible DEST_NODE route as shown in Figure 4.5.1. In [93], the author explains that this method is so dangerous and expensive that it provides a compelling reason to drop packets on MAL-Nodes. Therefore, it goes through the main options, even though it can direct to several fake claims.

Consider an RF attack scenario where SRC_NODE as *S* needs to send packets to DEST_NODE as *D* via the path "*S*→*N1*→*N2*→***M***→*N5*→*N8*→*D*". Node "*N2*" does not recognize the recognition of "*N5*" and transmits a packet to the MAL-Node "*M*" that should arrive at node "N5". This false communication directs to a path that does not have a path to DEST_NODE as "*D*", resulting in loss of packets transmitted. The result is that (1) all packets sent by the SRC_NODE are undetected and dropped by *M*, and (2) the legitimate node is unknowingly punished for packet loss. So, it concludes two cases of being categorized as malicious.

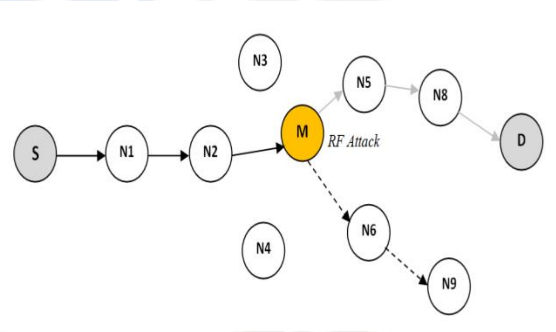


Fig4.5.1: RF communication scenario

IMED_NODEs can forever commence forged paths by changing data packets through information transmission, resulting in reduced throughput. The A-UPK captures changes in the data packet by encrypting the data packet with a particular UPK in transit. Both the SRC_NODE and the DEST_NODE create separate UPK for sending data packets to inform sensitive messages.

A-UPK creates a private key as AP_{UPKey} that uses the DH algorithm (DHA) for authentication and uses the hash algorithm to sign all messages sent during the node as MSG_{Sign} from RF attacks. A secure data packet as an EM_{RREQ} for broadcast is generated by the SRC_NODE as SN_{add} using the CA PUB_KEY, as shown under, where *RP* is the root path, D_{add} is the DEST_NODE address, and *TS* is the timestamp.

$$EM_{RREQ} = Enc(SN_{add}, MSG_{Sign}, MSG,\ AP_{UPKey}, RP, D_{add}\ , TS)_{CA_{pubkey}}$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.6982
***Article Received**: 02 April 2023 **Revised**: 15 May 2023 **Accepted**: 29 May 2023*

4.5.2 RF Attack Prevention Algorithm

To reduce RF attacks, A-UPK carries out reliable route identification and data routing. It performs the formation of a reliable route with a verification mechanism.

The A-UPK broadens the AODV route recognition method as shown in Figure 5.2 to provide a reliable and secure routing. The algorithm-1 illustrates the function of each method of the proposal A-UPK given below. Two methods for protecting the path identification *Init_RREQ*(D_{add}) and the destination response *nit_RREP* (SN_{add}) from RF attacks are described. The activities are performed by the IMED_NODE and the target node when they receive a secure and authenticated message during the route establishment procedure.

4.5.3 A-UPK simulation setup

The simulation was run for 600 seconds based on the parameters in Table 4.5.3. The node movement is randomly placed in the simulation area in the RWP model, with a pause time of 30 seconds and a speed of 5 m/s.

The simulation runs on multiple iterations and the number of MAL_nodes varies from 4 to 20. Here, 50% of the nodes are believed as source-destination pairs for the transmission nodes in the simulation. Transport packets are sent at a rate of 4 packets per second loaded into 512 bytes of information. Simulation results measure "PDR", "average E-2-E delay", "control overhead" and "packet drop rate" according to the fluctuations of the MAL-Node.

Table-4.5.3: Simulation Parameters

Configuration	Parameter Values
Simulation Area	1000m X 1000m
No. of Nodes	50
Pause Time	30 sec
Packet Size	512 bytes
CBR Rates	4 pkts/sec
Mobility	RWP
Mobility Speed (m/s)	5 m/s
Malicious Nodes	4, 8, 12, 16, 20

The simulation runs on multiple iterations and the number of MAL_nodes varies from 4 to 20. Here, 50% of the nodes are believed as source-destination pairs for the transmission nodes in the simulation. Transport packets are sent at a rate of 4 packets per second loaded into 512 bytes of information. Simulation results measure "PDR", "average E-2-E delay", "control overhead" and "packet drop rate" according to the fluctuations of the MAL-Node.

In this section we discuss the comparison analysis among the proposed methods in this research work. We compare Packet delivery, Control overhead and Packet drop ratio between RNBR, SAA and A-UPK.

The method of RNBR and SAA implements trust based measures to evaluate the security, whereas A-UPK implements authentication mechanism to secure the routing. Since, RNBR and SAA are based on the similar kind of measures, hence both so, a least variation in the packet delivery, control overhead and packet drop ratio. The result of A-UPK shows a better in compare to RNBR and SAA in average.

5.Result Analysis

A.Packet Delivery Ratio (PDR): It computes the ratio of the total number of information packets received at the DEST_NODE to the total number of information packets sent. It identifies the throughput performance of the protocol.

$$Packet\ Delivery\ Ratio = \frac{\sum Received\ Packets}{\sum Packets\ Originated}$$

Table-5.1: Packet Delivery Ratio comparison

MAL_NODE	RNBR	SAA	A-UPK
10	0.98	0.99	0.95
20	0.97	0.96	0.93
30	0.84	0.80	0.89
40	0.66	0.73	0.82
50	0.40	0.59	0.71

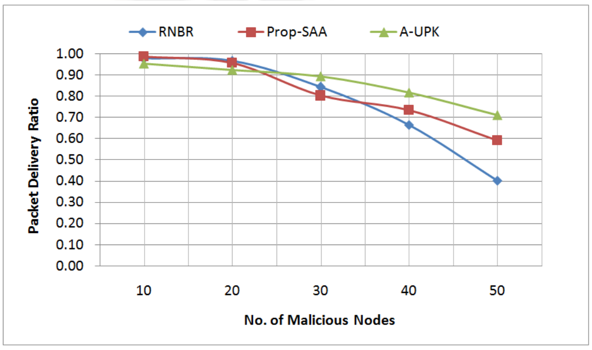


Fig5.1: Packet Delivery Ratio

Fig.1 shows the comparison of PDR between RNBR, SAA and A-UPK. The PDR result of SAA shows an average of 4% better PDR than RNBR and A-UPK in the presence least malicious nodes, but with increasing malicious nodes A-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.6982
***Article Received**: 02 April 2023 **Revised**: 15 May 2023 **Accepted**: 29 May 2023*

UPK shows better PDR. It achieves an average of 5% better PDR in compare to RNBR and SAA.

A. **Control Overhead:** It computes using the total number of control packets transmission and transmitted by the protocol during the simulation.

$$Control\ Overhead = \sum Number\ of\ Control\ Packets$$

Table 5.2: Control overhead Comparison

MAL_NODE	RNBR	SAA	A-UPK
10	2566	1566	5184
20	6526	4426	6187
30	15386	11486	6595
40	20110	15490	7443
50	23318	20318	9224

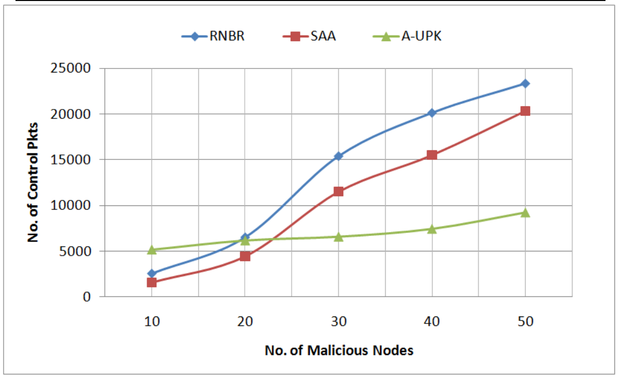


Fig5.2: Control overhead

Fig.2 shows the comparison of control overhead between RNBR, SAA and A-UPK. The control overhead of SAA and RNBR shows an average of 3% less control overhead in the presence least malicious nodes, but with increasing malicious nodes A-UPK shows better control overhead. It achieves an average of 10% low control overhead in compare to RNBR and SAA.

C.Packet Drop Ratio: It computes the percentage of the total number of packets dropped by a node during transmission over the link network.

$$Avg.Packet\ Drop\ Ratio = \frac{\sum Number\ of\ Packet\ Dropped}{No.of\ Nodes}$$

Table-5.3: Packet Drop Ratio comparison

MAL_NODE	RNBR	SAA	A-UPK
10	1950	1250	1125
20	2580	2410	1286
30	2980	2800	1422
40	4680	3980	2485
50	6521	5421	3099

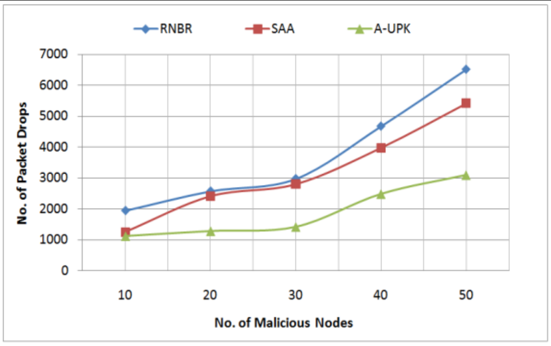


Fig5.3: Packet Drops

Fig.3 shows the comparison of packet drop between RNBR, SAA and A-UPK. The rate of packet drop is increased with increasing number of malicious nodes. A-UPK shows the least packet drops in compare to SAA and RNBR with an average of 2% less with SAA, and 3% less with RNBR at highest number of malicious nodes.

It concludes that the security methods based on trust attends more control overhead in compare to authentication based mechanism. It is due to the continuous evaluation of the trustiness of the nodes at runtime, whereas authentication mechanism attends an overload during initial authentication process later utilizing the credit of authenticity it reduce the overhead.

The loss of packets in case of RNBR and SAA is higher, due to the loss in the trustworthiness of a node at runtime can affects the data routing till the restoration of trust or utilizing the new route for the data routing, but the process and time complexity of these method is low, due to which it is most suitable for low computational, energy and storage devices. The authentication mechanism attains a slight higher process and time complexity but shows better PDR and low control overhead.

So, RNBR and SAA are best suitable for the situation where the energy, storage and processing capacity is low, and A-UPK can be utilizing where security is primary concern irrespective of the resource constraints.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.6982
***Article Received**: 02 April 2023 **Revised**: 15 May 2023 **Accepted**: 29 May 2023*

V. Conclusion and Future work

It concludes that the security methods based on trust attends more control overhead in compare to authentication based mechanism. It is due to the continuous evaluation of the trustiness of the nodes at runtime, whereas authentication mechanism attends an overload during initial authentication process later utilizing the credit of authenticity it reduce the overhead.

The loss of packets in case of RNBR and SAA is higher, due to the loss in the trustworthiness of a node at runtime can affects the data routing till the restoration of trust or utilizing the new route for the data routing, but the process and time complexity of these method is low, due to which it is most suitable for low computational, energy and storage devices. The authentication mechanism attains a slight higher process and time complexity but shows better PDR and low control overhead.

So, RNBR and SAA are best suitable for the situation where the energy, storage and processing capacity is low, and A-UPK can be utilizing where security is primary concern irrespective of the resource constraints.

REFERENCES

[1]. J. Loo, J. Lloret, and J. H. Ortiz, "Mobile Ad Hoc Networks: Current Status and Future Trends", Boca Raton, FL, USA: CRC, 2011.

[2]. I. Chlamtac, M. Conti, J. J.-N. Liu,, "Mobile Ad Hoc Networking: Imperatives And Challenges", Ad Hoc Networks, Vol. 1, pp 13–64, 2003.

[3]. Y. Ping, J. Xinghao, W. Yue, L. Ning, "Distributed Intrusion Detection for Mobile Ad Hoc Networks", Processing of the IEEE Symposium on Application and the Internet Workshops AINT-W05, 2005.

[4]. L. Butty'an 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.

[5]. S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks", in Proceedings of IEEE Infocom '03, San Francisco, CA, 2003.

[6]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in Mobile Computing and Networking, pp. 255-265, 2000.

[7]. S. Hariharan, N. Shroff, and S. Bagchi, "Secure Neighbor Discovery in Wireless Sensor Networks", Technical Report ECE 07-19, Purdue Univ., 2007.

[8]. J. P. Walters, Z. Q. Lian and W. S. Shi, "Wireless sensor network security: a survey", In Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, Boca Raton, Fla, USA, 2006.

[9]. A. Garg, A. Tiwari, H. K. Garg, "A Secure Energy Efficiency Routing Approach In Wireless Sensor Networks", International Journal of Engineering and Advanced Technology (IJEAT) , Volume-2, Issue-3, February 2013.

[10]. M. Chhabra, B. Gupta and A. Almomani, "A Novel Solution to Handle DDOS Attack in MANET", Journal of Information Security, Vol. 4(03), pp. 165-179, 2013.

[11]. S. S. Park, J. H. Lee, and T. M. Chung, "Cluster-based trust model against attacks in ad-hoc networks", in Third International Conference on Convergence and Hybrid Information Technology, pp. 526-532, 2008.

[12]. C. Dai, D. Lin, E. Bertino, and M. Kantarcioglu, "An approach to evaluate data trustworthiness based on data provenance", in SDM '08: Proc. 5th VLDB workshop on Secure Data Management, pp. 82-98, 2008.

[13]. Prof. Madhuri Zambre. (2016). Analysis and Modeling of Physical Stratum for Power Line Communication. International Journal of New Practices in Management and Engineering, 5(01), 08 - 13. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/42

[14]. D. Djenouri, L. Khelladi, N. Badache, "A Survey of Security Issues in Mobile Ad-hoc and Sensor Networks", Computer Journal of IEEE Communications Surveys and Tutorials, vol. 7, no. 4, pp. 1-15, 2005.

[15]. J. Wanga, Y. Liu, Y. Jiao, "Building a trusted route in a mobile adhoc network considering communication reliability and path length", Journal of Network and Computer Applications, Vol. 34, 1138-1149, 2011.

[16]. C. Lin and V. Varadharajan, "Modelling and evaluating trust relationships in mobile agents based systems", In Proceedings of the International Conference on Applied Cryptography and Network Security (ACNS'03), Lecture Notes in Computer Science, vol. 2846, pp. 176-190, 2003.

[17]. C. Xi, S. Liang, M. A. JianFeng, MA Zhuo, "A Trust Management Scheme Based on Behavior Feedback for Opportunistic Networks", Network Technology And Application, China Communications, 2015.

[18]. L. Buttyan and J.P. Hubaux. "Enforcing service availability in mobile adhoc wans". In Proceedings of IEEE/ACM Workshop on MANET and Computing Boston, MA, 2000.

[19]. A. K. Jain and A. Choorasiya, "Security enhancement of AODV routing protocol in mobile ad hoc network", In Proc. 2nd Int. Conf. Commun. Electron. Syst. (ICCES), pp. 958-964, 2017.

[20]. Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", to appear in ACM Wireless Networks (WINET), vol. 9, 2003.

[21]. J. Yan, J. Ma, F. Li, S. Moon, "Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks", Ad Hoc and Sensor Wireless Networks, vol. 10, pp. 235-251, 2010.

[22]. R. Lacuesta, J.Lloret, M.Garcia,andL.Penalver, "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation", IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 4, April 2013.

[23]. P. Giorgini, F. Massacci, J. Mylopoulos, and N. Zannone, "Requirements engineering meets trust management -

model, methodology, and reasoning", In Proceedings of the 2nd International Conference on Trust Management (iTrust'04), vol. 2995, pp. 176- 190, 2004.

[24]. Y. Chae, L. CingiserDiPippo,and Yan Lindsay Sun, "Trust Management for Defending On-Off Attacks ", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 4, 2015.

[25]. Y. Chae, "Redeemable reputation based secure routing protocol for wireless sensor networks", Master of Science Department Computer, University Rhode Island, Tech. Rep. TR12-331, 2012.

[26]. M. Yu, and K. K. Leung", A Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks", IEEE Transactions On Wireless Communications, Vol. 8, No. 4, 2009.

[27]. Pande, S. D. ., & Ahammad, D. S. H. . (2021). Improved Clustering-Based Energy Optimization with Routing Protocol in Wireless Sensor Networks. Research Journal of Computer Systems and Engineering, 2(1), 33:39. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/17

[28]. P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", Int. Conf. on 6th Joint Working Comm. Multi. Security, Pp.107-121, 2002.

[29]. K. Sanzgiri, B. Dahill, B. N. Levine, E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, November 2002, pp. 78-90.

[30]. Gaikwad, S. Y. ., & Bombade, B. R. . (2023). Energy Enhancement in Wireless Sensor Network Using Teaching Learning based Optimization Algorithm. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 52–60. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2507

[31]. A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision", Decis. Support Syst., vol. 43, no. 2, pp. 618-644, 2007.

[32]. W. J. Blackert, D.M. Gregg, A.K. Castner, E.M. Kyle, ,R.L. Hom and R.M. Jokerst, "Analyzing interaction between distributed DOS attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, pp. 26 - 36, 22-24 April, 2003.

[33]. Thomas, C., Wright, S., Hernandez, M., Flores, A., & García, M. Enhancing Student Engagement in Engineering Education with Machine Learning. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/123

[34]. M. Li, S. Salinas, P. Li, J. Sun, and X. Huang, "MAC-Layer Selfish Misbehaviour in IEEE 802.11 Ad Hoc Networks: Detection and Defence", Int. Journal of IEEE Trans. on Mobile Comp., Vol. 14, 2015.

[35]. J. Douceur, "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems, 2002.

[36]. J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis &Defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, pp. 259 - 268, 2004

[37]. D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks", IEEE Trans. Wireless Com., vol. 12, no. 9, pp. 4638-4646, Sep. 2013.

[38]. D. He, J. Bu, S. Chan, and C. Chen, "Handauth: Efficient handover authentication with conditional privacy for wireless networks", IEEE Trans. Computers., vol. 62, no. 3, pp. 616-622, Mar. 2013.

[39]. W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography", International Journal of Distributed Sensor Networks,DOI:10.1155/2013/730831, 2013.

[40]. L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network, Vol. 13(6), pp:24.30, 1999.

[41]. S. Hariharan, N. Shroff, and S. Bagchi, "Secure Neighbor Discovery in Wireless Sensor Networks", Technical Report ECE 07-19, Purdue Univ., 2007.

[42]. S. Yi, P. Naldurg, and R.Kravets. "Security-aware adhoc routing for wireless networks", In MobiHOC Poster Session, 2001.

[43]. S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta, and P. Dhurandher, "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems", IEEE Systems, Vol. 5, 2011.

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

[45]. Mohammad Hassan, Machine Learning Techniques for Credit Scoring in Financial Institutions , Machine Learning Applications Conference Proceedings, Vol 3 2023.

[46]. S. A. Thorat, P. J. Kulkarni, "Design issues in trust-based routing for MANET", In Proc. of International Conf. on IEEE Computing, Comm. and Networking Tech., 2014.

[47]. T. Jenitha, P. Jayashree, "Distributed Trust Node Selection for Secure Group Communication in MANET", In Proc. of International Conf. on IEEE 4th Advances in Computing and Comm., 2014.

[48]. P. Narula, S. K. Dhurandher, S. Misra, and I. Woungang, "Security in mobile ad-hoc networks using soft encryption and trust based multipath routing", Int. Journal of Science Direct Comp. Comm., Vol. 31, 2008.

[49]. F. Xing, and Wenye Wang, "On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures", IEEE Transactions On Dependable And Secure Computing, Vol. 7, No. 3, 2010.

[50]. E. M. Shakshuki, N.Kang, and T. R. Sheltami, "EAACK-A Secure Intrusion-Detection System for MANETs", IEEE Transactions On Industrial Electronics, Vol. 60, No. 3, March 2013.

[51]. Z. Wei, H. Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.6982
***Article Received**: 02 April 2023 **Revised**: 15 May 2023 **Accepted**: 29 May 2023*

Reasoning", IEEE Transactions On Vehicular Technology, Vol. 63, No. 9, 2014.

[52]. T. Shu and M. Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing, pp. 1536-1233, 2013.

[53]. H. Kozushko,"Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", Independent Study, Vol. 11. pp. 1-23, 2003.

[54]. T. Song, "Formal Reasoning about Intrusion Detection Systems", Computer Science.(n.d), p-1-206, 2007.

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