International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 5th Jan 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 01

DOI: 10.48047/IJIEMR/V12/ISSUE 01/27

Title **Trust Adaptability Model for Efficient Routing Based on Comprehensive Review over Manet Security Issues and Challenges**

Volume 12, ISSUE 01, Pages: 276-298

Paper Authors
M Venkata Krishna Reddy, P.V.S. Srinivas, M. Chandra Mohan

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Trust Adaptability Model for Efficient Routing Based on Comprehensive Review over Manet Security Issues and Challenges

M Venkata Krishna Reddy[1*], P.V.S. Srinivas[2], M. Chandra Mohan[3]
[1]Research Scholar, Department of CSE, Jawaharlal Nehru Technological University Hyderabad, Telangana, India &
Asst. Professor, Department of CSE, Chaitanya Bharathi Institute of Technology(A), Hyderabad, Telangana
Email: krishnareddy_cse@cbit.ac.in
[2]Professor, Department of CSE, Vignana Bharathi Institute of Technology, Hyderabad, Telangana, India
[3]Professor, Department of CSE, Jawaharlal Nehru Technological University Hyderabad, Telangana, India

Abstract
Security is considered as a major and essential research area in focus, and it engages in an essential task in achieving the success among the peoples and industrial in utilization through mobile ad hoc network. However, because of the limitations imposed by mobile nodes, it is struggling to get the trusted intermediary nodes for secure communication to the diverse targets to keep long network stability and preventing from active attacks. It is very necessary to identify the trusted intermediate nodes for high communication performance. Even though several combined security schemes are proposed for the MANETs, but they are not sufficient to provide a high-security performance using node trust identification based on the reliability and behavior prediction to enhance the security in MANET. This paper presents a review of the MANET security and Trust adaptability issues and challenges and discusses the constraints of MANET which affecting the security and adaptability with trust for security enhancement. Further, based upon the study carried on MANETs security and challenges, a novel trust based method for secure routing in MANETs using trust adaptability and transmission parameters is proposed in this article. Experimental results show that the proposed method, routing with trust computation is performing well when compared with existing routing protocol AODV without any trust calculation.

Keywords: Security, Trust adaptability, Secure Routing, MANET

Introduction

Wireless technologies and mobile devices development are an important and popular for information technology in different communication services and military-strategic environments to establish dynamic communication networks utilized to coordinate the military strategy between soldiers, vehicles and executive management locations. Small, mobile sensor nodes are able to communicate, perceive, and interpret data inside a larger network. These have a constrained transmission range and send data directly to the target[1]. Now a days Mobile Ad hoc Networks (MANET) are being part of many other heterogeneous networks including “Internet of Things (IoT)” and also includes other networks like ad hoc networks , wireless sensor networks and ZigBee. In present days, the usage of IoT devices has been increased significantly. The areas include homes, organizations, offices, industries etc.

In military environments, there are many risks that must be seriously considered due to the unique nature of MANETs, including an open wireless transmission medium, roaming and distribution network, and the lack of a centralized security protection infrastructure [2]. Therefore, security in strategic MANETs is a challenging research topic.

MANET is a "self-organizing" and "self-managed" wireless network with no infrastructure. Security in MANET is a major problem due to the lack of central infrastructure [3]. Trust and reliability reflect beliefs or trust or potential about the "honesty", "integrity", "competence", "availability" and "quality of service" of upcoming activities/behaviors of the target node. However, trust computations and management are extremely demanding in MANET because of the limitations in computational complexity and independent components in node mobility variation [4], [5].

Since wireless MANET contain dissimilar features from "wired networks" and "standard wireless networks", there is a need to address new challenges associated with security concerns. The level of trust computation required the understanding of trust definition, metrics, and calculations which are needs to be employed for the node trust and secure characteristics [6]. Since MANET cannot undertake centralized management or synchronization, because the application of

the network and their comparative positions change rapidly, and because the network is formed under cooperative efforts, these goals are more difficult to accomplish than traditional networks [7].

Security in MANET is a major problem due to the lack of central infrastructure [6]. Trust and reliability reflect beliefs or trust or potential about the "honesty", "integrity", "competence", "availability" and "quality of service" of upcoming activities/behaviors of the target node. However, trust computations and management are extremely demanding in MANET because of the limitations in computational complexity and independent components in node mobility variation [4], [5]. Since wireless MANET contain dissimilar features from "wired networks" and "standard wireless networks", there is a need to address new challenges associated with security concerns. The level of trust computation required the understanding of trust definition, metrics, and calculations which are needs to be employed for the node trust and secure characteristics [6]. Since MANET cannot undertake centralized management or synchronization, because the application of the network and their comparative positions change rapidly, and because the network is formed under cooperative efforts, these goals are more difficult to accomplish than traditional networks [7].

Security is one of the majority consistent areas of research and acts as an important function in influential the success of civil and commercial MANETs [8]. Unfortunately, due to the attacking model and the new type of adverse pattern, the security specification of the wired network cannot be directly returned to MANET. In other words, the mobile node is struggling to bring in trusted intermediaries to communicate with various targets. Trusted intermediaries are prerequisites for maintaining these communications active and liberated from aggressive attacks. This greatly impacts the advancement of security clarification at the routing layer, enabling secure "end-to-end services" among relevance to be implemented afterward having a reliable and secure routing layer.

So far, many security systems [9], [10] have been proposed for the MANET environment to protect routing nodes. Such as the "Watchers" is utilized in the environment propagating by "Link Routing Protocol". These are primarily utilized to detect the malicious behavior of network traffic-relied volatility and routers. However, it requires more

memory to keep records and counts for all routers. In MANETs, an untrusted node causes unbelievable harm and decreases the superiority and consistency of the data [11]. As a result, investigating the trust and reliability stage have the node results in a positive effect on the trust utilized to handle transactions with that node. Trust calculations are relatively simple in fixed networks, and the value of the trust varies mainly because of the behavior of the nodes. However, trust calculations are difficult in MANET because:

- The network composition may change significantly over time due to this mobility in an unpredictable manner. As the neighbour continuously transform, it happens to complex to supervise observations and get sufficient prospect for communications to determine the trust.
- If there is no "central control station", "monitoring the behaviour" of nodes is extremely complicated. The difficulty of trust calculations does not increase linearly exclusive of the central facility centre.
- Node behavior unpredictability among involuntary impermanent fault and deliberate malicious behavior of the "honest", "selfish" and "Malicious Node" which affects the on the whole trust of a node.

In general, the proposed secure routing protocols for MANET believe that every one node active in the network is co-operative and trustworthy, which may not always be true. To build a secure route it needs to implement some enhanced secure mechanism, which decreases the route-building overhead and usage of resources, as it required more computation for processing.

Wireless Mobile Adhoc Network

MANETs are wireless node system dynamically self-organizes into subjective and impermanent network topologies. It is able to internetwork people and vehicles in areas exclusive of pre-existing communications infrastructure or requiring the use of such infrastructure wireless extensions. At MANET, nodes able to interact directly with other nodes in their radio ranges; But non-interactive nodes are compatible with each other using the intermediate node [12]. In these cases, the nodes involved in the transmission automatically form a wireless network, so this type of wireless network able to establish the MANET.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The popularity of wireless communications and handheld devices has greatly promoted the development of wandering communications. These handheld mobile devices are self-organized in the nonexistence of infrastructure and the ability to enlarge their communications ahead of wireless transmission coverage may result in the development of MANET. A simple form of MANET network is shown in Figure 1.

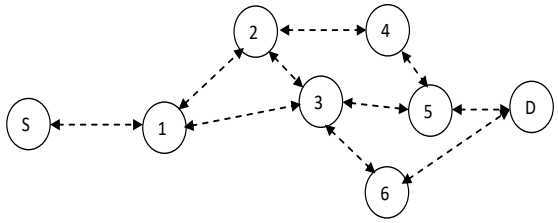

Fig.1. A illustration of MANET Network

Constraint of Mobile Adhoc Network

The Mobile ad hoc network (MANET) is considered as a dynamic network which creates a network exclusive of any infrastructure support. Its objective is to assist in dynamic scenarios where no infrastructure exists. Due to its repeated changing network topology, it faces many challenges in data routing and data security [16]. Mainly of the MANET routing protocols are supported by nature and implicitly trust on neighbor relations for the data routing.

Due to the constraints of many MANET routing protocols, the nodes in MANETS believe other nodes will constantly help with data transfer. This failure loses the possibilities of achieving the main power of the network having only one or two compromised nodes. The MANET are highly vulnerable to a variety of attack than wired relied on the network [17].

Literature Review

Manet Security Issues

MANETs distribute the essential security objective amid largely former networks. The security of MANET has become more prominent and the research requires serious attention from the community, availability, integrity, and privacy are the primary concerns of any secure wireless network [3] [13]. The necessitate for "Confidentiality", "Authenticity", "Integrity", "Availability", "Non-Repudiation" and "Access Control" is similar as in the erstwhile category of the networks and always principally resolute with the significance and compassion of applications utilized or data broadcasted. Several secure solutions have been presented for Mobile Adhoc networks, but most of these criteria and preventive technologies such as encryption, an authentication able to reduce the attacks, but hardly eliminate them.

A collaborative anomaly detection mechanism [18], [19] is implemented on each node that observes their neighbors independently. However, if a group of nodes is attacked is able to alert the innocent node. The "Watchdog" and "Pathrater" are designed for DSR routing protocols to detect network layer misbehavior [20]. Watchdog supervise the next-hop forward behaviour, but the "Pathrater" analyzes the results and chooses the most reliable way to deliver the packet. The scheme is restricted to source routing and is not effective against the significant node attack, especially the initial packet that is not recognized. This schemes [1] are limited to source routing and the packet cannot be detected efficiently against a significant node attack. However, the security level of wireless networks increases a certain limit by implementing IDS [21] relied on improved security algorithms relied on an "anomaly detection", "message cryptography" and "reliable or trust computation" for the supervision.

However, MANET cannot be centrally managed or coordinated, these goals are more difficult to accomplish than existing networks, as network participants and their relative status change rapidly and networks are formed through collaborative efforts.

The MANET's security-related research activities fall into three broad categories as follows:

(1). *Identification of nodes:* It must be able to identify the node of the MANET so that the nodes cannot spoof each other's identity. To avoid location profiling, it may be useful to use a pseudonym or a similar mechanism to protect personal information. The use of encryption keys, which offer more options for traffic data encryption, is frequently used to establish identity. Two major approaches are able to observe in the literature. In [22], the authors propose the threshold cryptography to produce a propagating certificate authority. Resultant threshold encryption shares secrets with the participants so that all participants can reconstruct their secrets. The distributed generation of public key pairs and distributed signing procedures are both supported by this schema variation. Another methodology completely nullifies the presence of the CA. In [23] suggests a plan to use a trusted web similar to the cryptographic tool PGP. All participants create their own public key pairs. When a participant is confident about another node's

identity, the participant signs the carrier's public key, which proves that identity of the participant. By following these links "A certifies the identity of B", the identity of a new node able to be checked.

(2). *Securing a routing protocol beside manipulations*: By means of different "cryptographic procedures", "manipulations" must be avoided by the routing process.

(3). *Preventing selfish behavior*: The motivation-based approach tries to encourage network client to aggressively contribute in MANET. The nodes may behave selfishly and maliciously due to the energy constraints in forwarding other nodes packets as they have to use their own energy. A representative scheme indicating this methodology as "Nuggets" by L. Buttyan et al. [24]. The author suggests initiated an essential exchange labelled having conveying strange traffic and transmitting their traffic. The main disadvantage of this methodology is that the trusted hardware must protect the identity.

The former methodology seeks to find and eliminate "selfish nodes" by S. Marti et al. [15]. The system utilized a "watchdog" that supervises the adjacent nodes to ensure if it, in reality, convey the data in forwarding to do, and the component will determine to avoid paths that enclose such misbehaving nodes.

Related Works in Security Enhancement Using Trust

MANET gathers nodes that creates an on demand network. Nodes are basically mobile and have limited resources. This is a packaged approach to numerous weaknesses and security attacks in MANET for search systems for both wired and wireless networks.

H. Kozushko et al. [25] have separated network IDs based on host, IDS is able to contradict two architectures. But, there is another type of IDS called Agent-based IDS. According to the host, IDS examines the system's status and looks for intrusions. It controls all the activities within the computer and any action that violates the security guidelines for the system should be reported. This network monitors the total network and its data flow traffic to detect unauthorized entry to the network. An "Agent - Trusted IDS" is a system that consists many independent agents, which are involved in finding malicious behavior in the network. All agents work mutually to identify infiltration activities.

J. Mundinge et al. [30] exploit the liar concept to analyze the reputation system utilized to detect intrusion in MANET. It has brought instructions for an efficient reputation system. A.P.Lauf et al. [31] suggested an implantable and propagating IDS through local analysis and comprehensive investigation to detect malicious nodes known as "HybrIDS". B.-C.Cheng et al. [32] presented a "context-adaptive IDS" that guarantees an intellectual trade-off among network existence and security. It utilizes the advance "Grammar programming" and another for the intrusion detection.

C.Xenakis et al. [33] made a good quality evaluation of the assessment and estimation of IDS. S. S. Zalte et al. [14] recommend an IDS, which is recognized as a "distributed court system", it is proven as a value in a situation such as extreme mobility and unfriendliness. J.-H.Cho et al. [34] suggested an "adaptive IDS" relied on "hierarchical group key management". F. Pakzad et al. [35] tried to present stages to progress the IDS in MANET using GA, it was also utilized for the IDS implementation.

C.M. Babu et al. [36] presented a "network-relied IDS" for MANET safety measures, it determined the network IDS that employed on gathering for "multi-classifiers" in sequence to distinguish intrusions. J.-H Cho et al. [37] presents TM considering the concepts such as dynamic trust, non-static, self-confidence, and trust are not necessarily transient, asymmetrical trust and trust depend on the context. At first, the group's trust was developed between the nodes using historical information and validation through the challenge process. From then on, the protocol generates confidence measures for other neighbor nodes based on social influencing factors like "friendship", "honesty", "privacy", etc., and in feature, updates are made continuously to build-up the trust track.

H. Xia et.al. [38] proposed a trust scheme for creating the finest trustworthy paths in particular route discovery. The trusts are categorized into the "historical", "current" and "route trusts". The Packets are separated by "control" and "data packets". The transmitting ratio of packets is based on "CFR (control packets forwarding ration)" & "DFR (data packets forwarding ratio)" computation and the outcomes are sustained in a "Trust record list" for every node. Trust value is calculated through a "fuzzy logic rules prediction" in view of the past standards and also using present standards of the node resources such as

"battery power", "local memory", "DFR", "CFR", "bandwidth", etc.

I. R. Chen et al. [39] incorporated "Social trust" and "QoS trust" and propose a procedure termed "SQTrust". The procedure was considered in such a way that the trust influenced is decreased and the functional performance is maximized. In such the "intimacy" and "honesty" is the community measures, whereas competency and acquiescence in QoS measures are being considered.

According to E. M. Shakshuki et al. [40] MANETS active and inadequate infrastructure escorts to severe difficulties in significant circumstances. To extend the security an "EAACK technique" is applied to overcome the constraints of "Watchdog technique" and also prevented the "fake acknowledgment packet" issues. It has the three most important measurements. First, it measures "end-to-end ACK scheme", where if an acknowledgment is not arriving then it identifies it as a misbehaving node in the path, and it transmits an ACK as "S-ACK (secure acknowledgment)" for switching to a new path. It secures the "S-ACK" by using a "Digital Signature" for encrypting the message to improve secure communication.

Material and Methods

Trust Computation Methods

Three elements make up trust computations: "experience," "recommendation", and "knowledge" [41]. Each node's "experience" component of trust is immediately assessed by its close neighbours and updated on a regular basis in the trust table. As part of the trust, the current trust table is recommended to all other nodes. The previously assessed trust is periodically included into the current 'knowledge' portion of total trust. Now, the trust can be calculated using either these three elements separately or in combination.

The following categories can be used to broadly group the work on trust computations:

- Distributed trust computations: Each node determines the value of trust it has in its neighbours.
- Centralized trust computations: Trust computations are managed and assisted by a central agent [41]

The research progress on these subjects are explained in detail below.

Amandeep Varma et al. [42], proposed the basic trust related security framework for Mobile ad hoc networks and the associated trust model. The method proposed is useful for the researchers having interest in trust model and trust

oriented framework for security in ad hoc networks.

In [43], a trust model is proposed which can be useful as a road map to carry out research work in the area of Trust adaptability Secure routing in Mobile adhoc Networks.

Muhammad Salman Pathan et al. [44] proposed a method to compute trust of a node by combining the social and QoS trust. Observations from this approach are mitigating nodes based on their packet forwarding ad receiving behaviour thus establishing a secure routing path.

Sethuraman et al. [45] given a trust management strategy that allows data packets transmission securely along the network with low energy consumption. In this solution a unique trust value is assigned to each node randomly. The integration of energy consumption and trust of every node is essential due to high node mobility. An algorithm is presented by Ahmed et al. where the calculation of trust is used to separate outbad nodes[46]. It was found that the proposed approach was useful for carrying out data transfer securely in mobile ad hoc networks.

A compound trust model which involves communal and QoS trust components is proposed by Jhaveri et al.[47] to calculate the degree of trust for the nodes in which social trust component called as the ditch ratio was used. This "ditch ratio" is useful for estimating the nodes performance while identifying misbehaving nodes.

In [48], algorithms are proposed for trust evolution of every node A trust calculation metric depending on Nodes behaviour to become malicious in dynamic scenario is given. Observation is that in this model, two type are trust are evaluated.In Ruo Jun Cai et al.[49], self detection and cooperative mechanism is proposed for trust evaluation.In [50], a method is presented to identify selfish nodes which could severely degrade the MANET performance. Here, Node reputation and path reputation is estimated by the source node for secure routing.In [51], Hui Xia et al. presented a dynamic trust based prediction model for evaluating trust worthiness of nodes, based on nodes historical behaviors and future behaviors estimated. Nodes Historical Trust is used to calculate Nodes Current Trust and Route Trust is calculated based on no of packets forwarded.

Lediona Nishani et al.[52] Machine Learning provided a survey on applying machine learning methods for Intrusion detection system in MANETs. Techniques

of Machine Learning can be adopted to detect the activities of a node normal or abnormal.

In [53], provided a new model to detect malicious nodes using reinforcement learning that enhances the security.

Waleed Alnumay et al.[54] A Trust Based Model IoT proposed a novel model for IoT-MANET Clustering Environment. It computes the resultant trust of a node by using Direct and Indirect Observations. The deployment geography, applications, degree of infrastructure available, and level of precision required can all influence the choice of trust computation algorithms. The deployment geography, applications, degree of infrastructure available, and level of precision required can all influence the choice of trust computation algorithms. Distributed calculations are accurate and do not have a single point of failure, but they are biassed and not global in nature. Centralized trust calculations, on the other hand, have a single point of failure despite being global. Table 1 includes a full comparison of the various trust computation methods along with the pertinent references used in this study.

3.2 TRUST PROPAGATION

If the computed trust spreads throughout the network after being computed on target by one of the nodes, the resources required to compute trust again by other nodes might be decreased. For instance, node A can really bypass the explicit trust computation on node X if node A learns the trust value of node X from nodes B and C. This is crucial in MANETs since they have limited infrastructure, autonomy, mobility, and resources. The simplest example of trust propagation is recommendation.

Table 1. Comparison of different trust computing mechanisms

Authors and year	Context in use	Trust and Performance Metrics	Advantages	Complexity and Limitations	Scope
Lenin Guaya-Delgado Pathan et. Al, 2019 [50]	Dynamic Reputation Based Algorithm for Computing Node Reputation for secure Routing	Node Reputation is computed according to their packet forwarding behavior	Simple Trust Computation based on Packet Forwarding Behavior. Path reputation is also measured depending on packets forwarded and received at Destination.	Estimates the Nodes reputation by sharing the losses among the nodes equally that form the path so genuine node and selfish node are treated in same way	Node Reputation and Path Reputation using packet forwarding behavior
Waleed Alnumay et. Al, 2019	Trust based predictive Model for MANETS in	Detection of Good and Bad Node based on their packet	Parameters considered are based purely on packet forwarding	Complex calculations for Trust computation	Resultant Trust Calculation based on Direct and Neighbor

[54]	Internet of Things and secure Routing	forwarding behavior	behavior		Trust
Muhammad Salman Pathan et. Al, 2018 [44]	Trust Computation using Neighbor Observations along with QoS Parameters	Trust is measured depending on Packet forwarding behavior and QoS Parameters	Various QoS Parameters are used to compute Neighbor Trust	QoS Parameter like Channel Quality may be complex to calculate in MANETs	Neighbors Trust using QoS Parameters and Packet Forwarding Parameters for Trust Computation, Intelligent prediction functions can be used for evaluating nodes capability
Ruo Jan Cai et. al, 2018 [49]	An Evolutionary Self Cooperative Trust Computing Scheme was proposed	Trust is computed based on Self Detection and Cooperative Detection using record maintenance like SHR, RHR, SAR, NJR etc.	Self Detection and Cooperative Detection	Maintenance and Update of various records time to time for evaluating Trust	Combination of Self and Cooperative Trust Computation, Usage of Records to some extent
Hansi Mayadunna et. al, 2018 [53]	Reinforcement Learning is adopted to find misbehaving nodes in MANETS	Direct and Indirect Trust values are computed based on several parameters. Further Reinforcement learning is adopted to classify malicious nodes	Total eight parameters are used to compute Node Trust directly and Indirectly	Structure of Q Table and its maintenance as part of Reinforcement learning	Parameters can be considered for Trust computation for more accuracy and efficiency along with Reinforcement learning
Lediona Nishani, et. al, 2016 [52]	Use of Machine Learning for detecting intrusions in MANETs	Anomaly Based IDS in MANETS identifies the attack behavior diverges from the normal behavior	Techniques of Machine Learning are applied to predict the difference between the baseline normal behavior and the newly happened event	Classification approaches are not clearly addressed	Machine Learning Techniques can be used to predict nodes behavior based on the present performance.
KefayatUllah, et. al, 2015 [48]	Trust Model for Node Authentication in MANETS using Direct and Indirect measures	Blind Trust and Reference based Trust are used for Trust Computation	Combination of Blind and reference Trust is used	No Proper parameters to calculate Trust value	Relationship Equation for combining the Blind and Referential Trust and Threshold values to make a decision on Node authentication

The closest direct neighbor provides the majority of recommendations. However, trust propagation may include multiple hops. The transitivity attribute of trust is the foundation for trust propagation. Cooperation in the network for transferring the trust information is the primary factor to be taken into account for trust propagation. The majority of nodes should collaborate in conveying the trust information, if not all of them.

MANETs are networks that are very dynamic. In this network, connectedness, neighborhood, and associations are always

changing, which has an impact on trust and its dynamics. Mobility, network density, and connection failures are a few examples of network dynamics.

Proposed Method

From the above study and review on various trust computation and route security mechanisms, the following observations are made.

1. Source initiates data transfer to the destination directly if it is in the range of source. But if the destination is out of reach from the source, then source data transport must rely on intermediary nodes.

2. A node has to dissipate its own energy while transferring the data packets in MANETs. If intermediate nodes hesitate to use/lost their energy for transferring other node's data packets then they behave maliciously/selfishly and drop the packets. Thus effects the secure data transfer and secure routing in MANETs.

3. All the existing security mechanisms based on cryptography and signature method fails to address the identification and isolation of malicious nodes from routing. This strengthens the concept of trust based secure mechanism in MANET routing for secure data transfer. Isolation of malicious nodes during routing is essential for reliable communication from source to destination.

4. Trust based routing mechanisms enable routing and data transfer only after computing nodes trust, deciding the nodes behavior whether malicious or not, then involving only the trustworthy nodes in routing thus isolating the malicious nodes and performing secure routing.

5. It is observed from the above review that all the proposed and existing trust based routing mechanisms are computing node's trust without considering node's behavior and network parameters.

The proposed method in this paper computes the node's trust based on direct observations considering network parameters and node's behavior. Routing Decision is made depending on the Node Categorization whereas Node categorization depends on Trust calculation.

Trust Calculation

Node A wants to calculate trustworthiness of Node B which it wants to include as inter mediatory node for routing data packets to the destination. Node A initiates trust calculation on Node B. Due to the distributed nature of Mobile ad hoc Networks, a node can monitor neighbor node to evaluate its behavior during their direct communications in a passive mode.

Algorithm (Trust Dependent Approach-TDA)*:*

Procedure for computation of Direct Trust(DRT, ND1, ND2, DPFR)

//DRT is the Direct Trust

//ND1 is the node and ND2 is its neighbor node

//Ratio of Data packets forwarded, DPFR

//Direct Trust DRT

{

Step 1: The process begins if any node starts finding for trustworthiness in a neighboring node.

Step 2: Data Packet Forwarded Ratio is calculated as

$$DPFR = w_1 *(D_f/ D_t) + w_2 *(D_d/ D_t)$$

Step 3: Then Direct Trust, DRT is calculated from

$$DRT = w_1 * DPFR$$

}

end procedure

Direct Trust Calculation:

Direct trust related values *DRT* of neighbor nodes by applying the below network parameters.

1. The node's total number of data packets received $=D_t$
2. Number of data packets sent by the node correctly $= D_f$
3. The number of dropped data packets by the node $= D_d$

Node A collects the information regarding above network parameters for calculating trust by observing traffic that goes through the each neighbor of Node B. Then 'Node A' uses the above information to calculate direct trust value in a time period τ_{Time}. After running out of each time period τ_{Time}, the trust parameters are gathered again and direct observation "*DRT*" is evaluated. Because MANETs are dynamic, trust is calculated on a regular basis. Nodes are categorized according to their positive and negative character by comparing them to the Trust threshold.

After gathering the information using above network parameters regarding the node, the Data packets ratio can be calculated by Node A on Node B using Equation 1.

Data packets forwarded ratio, DR

$$DPFR = w_1 *(D_f/ D_t) + w_2 *(D_d/ D_t) \quad (1)$$

Where $w_1 + w_2 = 1$

Where w_1, w_2 are the corresponding weights

Final Direct trust calculation of a node is done based on Data packets forwarded ratio using Equation 2

DRT = Direct Trust , $DRT = w_1 * DFR$ (2)

Where $w_1 <= 1$

After computing the Direct trust *DRT*, the nodes are clustered into two groups

Good or Bad, depending on their Direct Trust evaluated using Equation 2 and compared with Static trust Threshold TH. These threshold limits are fixed depending on network configuration.

$$\textit{Good:} \text{ if } DRT \geq TH$$
$$\textit{Bad:} \text{ if } DRT < TH$$

Source finds trusted nodes using the proposed scheme to establish the secure route to destination. Each node consists the list of dependable(trusted) neighbour nodes as well as their latest trust values calculated. At this point, the source-to-destination path is formed by considering only good nodes.

Simulation and Results

The suggested trust-based solution's effectiveness is demonstrated by contrasting it with the current routing protocol, which uses intermediate nodes without doing any prior trust computations. A node's direct trust value is determined using a proposed scheme in this study by looking at how it transmits data. Various transmission parameters like number of data packets forwarded or dropped are considered for the direct trust calculation. In this proposed solution, the resultant trust is evaluated using a computable approach by considering the direct trust observations of the Node using network parameters. A 700 m2 x 500 m2 network space is used for simulation, and IEEE 802.11 MAC for 500s with 22 nodes is employed. In the simulation, it is seen that good nodes lose data packets as a result of network environmental conditions such as node mobilization, packet collisions, etc., but malignant or selfish nodes purposefully lose data packets. The simulation parameters are summarized in Table 1.

Table 2 Parameters used for Simulation

Parameter	Value
Simulator used	NS2.34
Nodes number	21
Area of Network	700 x 500
Size of the Packet	512 bytes
malicious nodes	05
Type of the Traffic	CBR/UDP
Mobility	4–25 m/s
Pause Time	5s
Time for Simulation	500s

Results

Results are examined after conducting the simulation. Using the proposed method – Direct Observations, node's trustworthiness is evaluated. Results generated and computations carried out for direct trust computation from the simulation are tabulated in Table 2.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Table 3. Malignant Nodes detection and removal

Node	Direct Trust	Static Trust Threshold	Classification
Node 1	0.7234	0.5	Good
Node 2	0.62354	0.5	Good
Node 3	0.32567	0.5	Bad
Node 4	0.54123	0.5	Good
Node 5	0.19675	0.5	Bad
Node 6	0.56843	0.5	Good
Node 7	0.67423	0.5	Good
Node 8	0.5212	0.5	Good
Node 9	0.52178	0.5	Good
Node 10	0.35162	0.5	Bad

Static Threshold value is fixed as 0.5 for all the nodes based upon Network conditions.

Performance Evolution and Discussion

Metrics like Packet Delivery Ratio (PDR), Detection of False Positives, and Throughput are taken into consideration for the proposed scheme's performance evolution.

False Positives Detection Ratio :

Calculating "False positive" involves dividing the number of good nodes that were mistakenly classified as harmful by the total number of nodes available in the network. Figure 2 plots the proposed scheme's false positive detection rate against the fraction of packets that collided. The graph below demonstrates that only 5.4% of nodes are falsely identified as malicious when 25% of packet collisions take place.

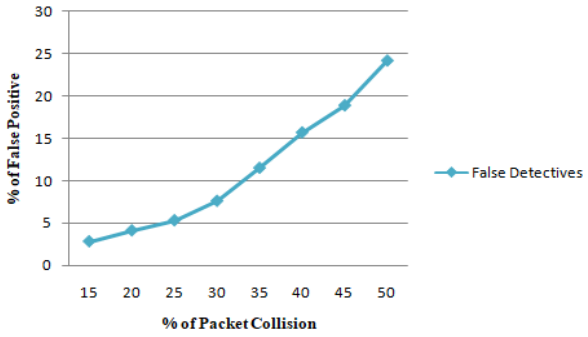

Fig. 2. False Positive Detection Ratio

Packet Delivery Ratio:

Fig. 3 illustrates how the presence of malicious nodes affects packet delivery. The proposed solution is compared to the current routing protocol without trust, AODV in the graph. The high packet delivery ratio is clearly demonstrated. The current routing protocol's packet delivery ratio for 5% of malicious nodes is 69 packets per second, while the suggested scheme's packet delivery ratio is 82 packets per second. It is observed that in proposed scheme detecting malicious nodes using trust evaluation and avoiding them in routing increased the packet delivery ratio.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

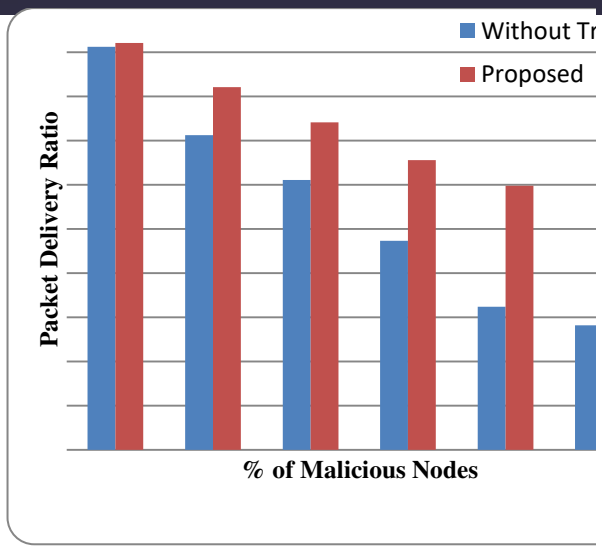

Fig. 3. Packet delivery ratio mapped with number of malicious nodes.

Throughput:

The throughput comparison between the suggested technique and the present routing protocol without trust computation, AODV is shown in Fig. 4. Throughput is number of units delivered in stipulated time. The graph below demonstrates that the current routing protocol, which does not compute trust, delivers 492 packets on average in 6 seconds whereas the proposed system, which computes trust, delivers 591 packets on average in 6 seconds. It demonstrates how effective the suggested strategy is in terms of throughput.

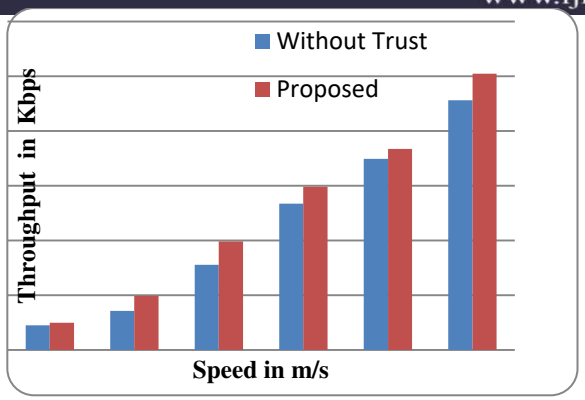

Fig. 4. Throughput comparison

Conclusion and Future Research Prospective

The widespread application of MANET is open for wide security focus due to the open nature of communication. MANETs are vulnerable in their performance. Intruders able to negotiation network operations by attacking "physical", "MAC", or "network layers". The network layer, in particular, the routing protocol, is susceptible due to the utilization of supportive routing algorithms, the inadequate computational capability of nodes, the drain out node energy and the lack of specific physical network boundaries and the momentary nature of services in the network.

Future research works will able to provide solutions to security challenges in MANET using trust-building methods. Trust is a key component of MANET. It enables components to handle uncertainty and degradation created by others. This motivates us to present novel protocol

relied on a node trust computation and Node Behavior Prediction for effective trust management , quality of service and secure routing. This involves the following development as follows through,

- Exploring the current security concern in MANET Networks in data routing,
- Discovers the challenges in security Systems in MANET and the influence of trust relied on prevention,
- And providing an insight into the current "Trust estimation" and "Reliable Node predictions" for efficient throughput and secure routing in MANET.
- Providing Secure Routing in MANETS with Trust adaptability approaches in Node Categorization.

After the review on security issues and challenges in MANETs and study of various trust computing mechanisms, it is observed that a more comprehensive road map for secure routing involving trust may be required. A comparison between existing trust computation methods is shown in table 1. New trust mechanisms for identifying trusted nodes required for secure routing. The following proposals are made for secure routing in MANETs by adapting trust.

1. Trust should be calculated based on both direct and indirect observations of nodes in the network. This can be extended to 2-hop neighborhood.

2. Trust should be computed by considering the network parameters that change dynamically time to time.

3. Adaptive trust threshold should be evolved based on network parameters.

4. The efficiency of proposed trust method should be evaluated with network parameters like node linkage.

5. Routing between source and destination can be done only by considering trust nodes evaluated as intermediately nodes.

This article presents a review on MANET security concern in relevance to trust adaptability. It primarily discusses the characteristics and constraints of MANET in terms of data routing. It presents an insight on MANET security issues and challenges for the identification of malicious nodes. Trust-based security in MANET provides a foremost advantage to dynamically detect the misbehaviors. We discuss the security mechanisms using trust in IDS to detect the anomaly detection of the malicious nodes. In related, it discusses the trust management schemes, various trust computation methods and the related works presented to enhance the security in MANET. The utilization of trust in MANET security can further be enhanced to provide an adequate

low overhead routing algorithm in future works.

In this article, based on the study conducted, a trust based approach is proposed for secure routing. Nodes Trustworthiness is evaluated based on direct observations considering network parameters and node's behavior. Secure Data transmission is enrooted between source and destination involving only trustworthy nodes and isolating the misbehaving nodes using the proposed approach.

Acknowledgment

We would like to express our gratitude and appreciation to all of the members for their ongoing support.

REFERENCES

[1] Gayathri, S., and A. Senthilkumar. "Energy efficient based secure data transmission for multi hop trust management technique using wireless sensor network." ictactjournals.in, Vol. 12(4), 2021.

[2] J. -H. Cho, H. A.-Hamadi, I.-R. Chen, "COSTA: Composite Trust-Based Asset-Task Assignment in Mobile Ad Hoc Networks", IEEE Access, Vol. 7, 2019.

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

[4] M. Chatzidakis, S. Hadjiefthymiades, "Location-Aware Clustering and Trust Management in Mobile Ad Hoc Networks", IEEE 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2018.

[5] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, "Security and trust management in opportunistic networks: A survey", Security and Communication Networking, vol. 8(9), pp. 1812-1827, 2015.

[6] N. Asai, S. Goka, H. Shigeno, "A Trust Model Focusing on Node Usage in Mobile Ad Hoc Networks", IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2019.

[7] P. B. Velloso, R. P. Laufer, D. D. O. O. Cunha, O. C. M. B. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model", IEEE Trans. Netw. Service Manag., vol. 7(3), pp. 172-185, 2010.

[8] 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, Volume: 18, Issue: 2, Pages: 1287 - 1309, 2016.

[9] 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", International Journal of IEEE Systems, Vol. 5, No. 2, 2011.

[10] Y. Wang, I.-R. Chen, J.-H. Cho, A. Swami, and K. S. Chan, "Trust-based

service composition and binding with multiple objective optimizations in service-oriented mobile ad hoc networks", IEEE Trans. Services Comput., vol. 10(4), pp. 660-672, 2017.

[11] H. -S. Yang, Seung-Jae Yoo, "Authentication Techniques for Improving the Reliability of the Nodes in the MANET", IEEE 2014.

[12] G. Vaseer, G. Ghai, D. Ghai, P. S. Patheja, "A Neighbor Trust-Based Mechanism to Protect Mobile Networks", IEEE Potentials, Vol. 38(1), 2019.

[13] M. Raya, J.-Pierre Hubaux, "The security of vehicular ad hoc networks", In Proceedings of the 3rd ACM workshop on Security of Ad hoc and Sensor Networks (SASN'05), pp. 11-21, 2005.

[14] S. Campadello, "Peer-to-peer security in mobile devices: A user perspective", In Proceedings of the 4th International Conference on Peer-to-Peer Computing (P2P'04), pp. 252-257, 2004.

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

[16] D. Wang, T. Muller, Y. Liu, J. Zhang, "Towards robust and effective trust management for security: A survey", In Proc. The 13th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom), 2014.

[17] J. Cho, K. Chan, S. Adali, "A survey on trust modeling", ACM Computer Survey, vol. 48, no. 2, p. 28, Nov. 2015.

[18] R. Mitchell, I.-R. Chen, "A survey of intrusion detection in wireless network applications", Computer Communication, vol. 42(3), pp. 1-23, 2014.

[19] Z. M. H. Islam, A. A. Khan, "Detection of dishonest trust recommendations in mobile ad hoc networks", In Proc. 15th Int. Conference Computing, Communication and Networking Technology (ICCCNT), pp. 1-7, 2014.

[20] M. A. Ayachi, C. Bidan, T. Abbes, 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.

[21] S. S. Zalte, V.R. Ghorpade, "Intrusion Detection System for MANET", IEEE 3rd International Conference for Convergence in Technology (I2CT), 2018.

[22] J. -H. Cho, I.-R. Chen, S. J. Kevin, "Trust threshold-based public key management in mobile ad hoc networks", Elsevier Ad Hoc Networking. Vol. 44, Pp. 58-75, 2016.

[23] M. N. Ahmed, A.H. Abdullah, H. Chizari, O. Kaiwartya, "Flooding Factor-based Trust Management Framework for secure data transmission in MANETs", J. King Saud Univ. Comput. Inf. Sci., 29, 269-280, 2017.

[24] L. Buttyan, 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.

[25] H. Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion

Detection Systems", Independent Study. 11 (n.d), p-1-23, 2003.

[26] C. Lin, 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.

[27] X. Wang, K. Govindan, P. Mohapatra, "Provenance based information trustworthiness evaluation in multi-hop networks", in IEEE Global Communication Conference, Globecom-10, 2010.

[28] D. McCoy, D. Sicker, D. Grunwald, "A mechanism for detecting and responding to misbehaving nodes in wireless networks", in 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON '07, pp. 678- 684, 2007.

[29] V. Balakrishnan, V. Varadharajan, P. Lucs, U. K. Tupakula, "Trust enhanced secure mobile ad-hoc network routing", in 21st International Conference on Advanced Information Networking and Applications Workshops, AINAW '07, pp. 27-33, 2007.

[30] J. Mundinge, J.-Y. Le Boud, "Analysis of a reputation system for Mobile Ad-Hoc Networks with liars", Elsevier, 65 (n.d), pp. 212-226, 2008.

[31] A. P. Lauf, R. A. Peters, W. H. Robinson, "A distributed intrusion detection system for resource-constrained devices in ad-hoc networks", Elsevier, 8 (n.d), pp. 253-266, 2010.

[32] B. -C. Cheng, Ryh-Yuh Tseng, "A Context Adaptive Intrusion Detection System for MANET", Elsevier. 34 (n.d), p-310-318, 2011.

[33] C. Xenakis , C. Panos, I. Stavrakakis , "A comparative evaluation of intrusion detection architectures for mobile ad hoc networks", Elsevier, 30 (n.d), p-63-80, 2013.

[34] J. -H. Cho, Ing-Ray Chen, "Performance analysis of hierarchical group key management integrated with adaptive intrusion detection in mobile ad hoc networks", Elsevier, 68 (n.d), p-58-75, 2011.

[35] F. Pakzad, M. K. rafsanjani, A. B. Saeid, "The improvement steps of intrusion detection system architecture of MANET", Mathematics & statistics. 22 (n.d), p-1-13, 2011.

[36] C. M. Babu, U. A. Lanjewar, C. N. Manisha, "Network Intrusion Detection System On Wire Less Mobile Adhoc Networks", IJARCCE Vol. 2, P-1495-1500, 2013.

[37] J. -H. Cho, A.N, Ananthram Swami A, Ing-Ray Chen B, "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks", Elsevier, p1001-1012., 2012.

[38] H. Xia , Z.Jia , Xin , Lei Ju , Edwin H.-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks", Elsevier, Vol-11, p-2096-2114, 2013.

[39] I. -R. Chen, J. Guo, F. Bao, J.-H. Cho, "Trust management in mobile ad hoc networks for bias minimization and application performance maximization", Elsevier, p-59-74, 2014.

[40] E. M. Shakshuki, N. Kang, T. R. Sheltami, "EAACK-A Secure Intrusion-Detection System for MANETs", IEEE Vol. 60, p-1-10, 2013.

[41] Kannan Govindan, Prasant Mohapatra, "Trust Coputations and Trust Dynamics in Mobile Adhoc Networks : A Survey", IEEE Communications Surveys & Tutorials , Vol. 14(2), 2012.

[42] Amandeep Verma, Manpreet Singh Gujral, "Trust Oriented Secure Adhoc Networks : A Generic Framework", International Journal of Emerging Technologies in Computational and Applied Sciences , Vol. 5(5), 2013.

[43] Venkata Krishna Reddy M, Dr. R.Ravinder Reddy, " A Trust Based Method for Providing Secure Data Transmissions in Mobile Ad hoc Networks", International Conference on Emerging Trends in Circuit-branch Technologies and Applications, 2021.

[44] Muhammad Salman Pathan, Nafei Zhu, Jingsha He, Zulfiqar Zardari, "An Efficient Trust-Based Scheme and Quality of Service Routing in MANETs", MDPI-Future Internet , Vol. 10(16), 2018.

[45] Sethuraman, P.; Kannan, N. Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. Wirel. Netw. 2017, 23, 2227–2237.

[46] Ahmed, M.N.; Abdullah, A.H.; Chizari, H.; Kaiwartya, O. Flooding Factor based Trust ManagementFramework for secure data transmission in MANETs. J. King Saud Univ. Comput. Inf. Sci. 2017, 29, 269–280.

[47] Jhaveri, R.H.; Patel, N.M.; Jinwala, D.C. A Composite Trust Model for Secure Routing in Mobile Ad-Hoc Networks. In Ad Hoc Netw.; Ortiz, J.H., de la Cruz, A.P., Eds.; InTech: London, UK, 2017; ISBN 978-953-51-3109-0.

[48] KefayatUllah, Rajib Das, Prodipto Das, Ananya Roy, "Trust and Secured Routing in MANET : An Improved Approach", International Symposium on Advanced Computing and Communication , 2015

[49] Ruo Jan Cai, Xue Jun Li, Peter Han Joo Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs", IEEE Transactions on Mobile Computing , 2018.

[50] Lenin Guaya-Delgado, Esteve Pallares-Segarra, Mezhar, Jrdi Forne, "A Novel dynamic reputation-based source routing protocol for mobile ad hoc networks", EURASIP Journal on Wireless Communications and Networking , 2019

[51] Hui Xia, Zhiping Jia, Xin Li, Lei Ju, Edwin H.-M. Sha, "Trust Prediction and trust-based source routing in Mobile Adhoc Networks ", Ad hoc Networks, Vol. 11, 2013.

[52] Lediona Nishani, Marenglen Biba, "Machine Learning for Intrusion Detection in MANET: a state-of-the-art-survey", J Intel Inf Syst , 2016.

[53] Hansi Mayadunna, Shaneen Leen De Silva et al., "Improving Trusted Routing by Identifying Malicious Nodes in a MANET Using Reinforcement Learning", International Conference on Advances in ICT for Emerging Regions , 2017.

[54] Waleed Alnumay, Uttam Ghosh, Pushpita Chatterjee, "A Trust-Based Predictive Model for Mobile Ad Hoc

Network in Internet of Things", MDPI-Sensors , Vol. 19, 2019.

[55] M. J. Probst and S. K. Kasera, "Statistical trust establishment in wireless sensor networks," in Proc. 13th International Conference on Parallel and Distributed Systems, pp. 1–8, 2007.

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