International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-8, June 2020

An Outline on Issues in Efficient Trust Supervision in Mobile Ad Hoc Networks

M.Anugraha, S.H.Krishnaveni

Abstract*: Mobile Ad hoc Network is an assortment of free hubs that can convey one another. These hubs are self-composed hub, which doesn't have any fixed framework like base station, radio wires, and so forth. The hubs with in its range can have an immediate correspondence if not it utilizes a moderate hub for transmitting the information. Each node will act as both host and router. The nodes can join or leave the network anytime and makes the network topology. Network topology is dynamic in nature. Because of the dynamic behavior the detection of trust value is difficult for intermediary node. Trust should be managed in the network ie., the network has different behaviors like malicious, selfishness, unhealthiness, etc., due to these behaviors the trust of an intermediary node is difficult to calculate. Right now safe routing is performed by the improvement of convention which yields the minimization of trust inclination and boosts the application execution. This study compares different trust management framework and compare the trust level based on the metrics and outlines the issues and future ideas.

Keywords* : *Mobile Ad hoc Network, Dynamic topology, Intermediate nodes.

I. INTRODUCTION

Mobile Ad hoc Networks are self-sorted out cell phones. Every hubs go about as host and switch and doesn't have any fixed foundation like reception apparatuses, base station and so forth. The hubs in the system are dynamic in nature; they move arbitrarily and make another connection with different gadgets. The serious issue in MANET is powerless assaults. To actualize a particular capacities like directing and security the imparting hubs in MANET ought to help out one another and every hub go about as transfer hub varying. At the point when a hub attempts to send data to different hubs which is out of its correspondence go, the data must to be sent through more than one node. The MANET has considerable constraints like bandwidth, computer power and battery power. The neighbor node will not act well as every time it will be selfish or malicious during sometimes. Due to this misbehavior the data flow will be affected in the network.

Trust the executives are reciprocally utilized with reputation management. Trust in a hub's conviction dependent on the trust characteristics and the reputation is feeling about a hub.

Revised Manuscript Received on June 30, 2020.
***** Correspondence Author
M.Anugraha*, Computer Science and Engineering, Noorul Islam University, Nagercoil, India. Email: grahaanu90@gmail.com
Dr.S.H.Krishnaveni, Computer Science and Engineering, Baselios Mathews II College of Engineering, Kollam, India. Email: shkrishnaveni@gmail.com

Trust the board incorporates foundation ie., gathering fitting trust confirmations, trust collection, trust dissemination, trust revelation and assessment of trust evidence. The primary impression of trust the executives is arrangement creator. Disseminated trust the board structure was first analyzed in trust the executive's issue. It will provide the third party certificate for a trust security. Trust management is aimed to provide a relation between nodes in a malicious network.

In MANET, the nodes are in distributed manner, in which the nodes are out of its range chooses an intermediate node for transferring the data. So the intermediary node should be true to source and the destination. So the trust value should be calculated in a network. Trust is characterized as a proportion of abstract conviction, that one individual play out a promising activity before the possibility present itself to analyze whether the activity has happened. Trust is characterized as a proportion of emotional conviction, that one individual play out a promising activity before the possibility present itself to inspect whether the activity has happened. The trust commendable is an individual that the normal activity is acted in the way that ought to be promising to the trustor.

Hybrid Trust Model (HTM) was proposed in MANETs; here advancement system is utilized that is Ant Colony Optimization (ACO) [32, 35]. This ACO calculation finds the most limited way from source hub to neighbor hub. ACO calculation gives key to every single hub.

By giving key [33, 37] to every hub, the hubs are safely kept up. The key age additionally assists with maintaining a strategic distance from the information duplication, information drop, and so on. The ACO calculation will send the information individually so it will take some multiple occasions to convey the information. So as to control the time, DSR directing convention [35, 37] was utilized. DSR keeps up channel and passage. First the hubs will send the information to the channel.

The channel will check whether the hubs are approved are definitely not. In the event that it is approved the hubs send the information through the door, with the goal that the time is additionally devoured and the information is likewise safely kept up. Here the hubs will send the bundle to the goal through the middle hub in a participate way. So the expectation of trust in moderate hub is troublesome.

By estimating a portion of the parameter like availability, vitality, unselfishness, fitness the trust can be anticipated in a hub. This paper surveys different trust based protocols which obtains the trusted routing in selfish and malicious affected node in a network. This paper proceed as follows, section I introduction, section II survey on trust management, section III discussion on algorithms, section IV concludes the paper and outlines the future work.

II. SURVEY IN TRUST MANAGEMENT

A. Partially distributed dynamic model

This work was presented by Anjali Anand, Himanshu Aggarwal [29].

A Partially distributed dynamic model is proposed to enhance the security of network. This proposed system at different time various attackers are determined. Thus the nodes undergo a dynamic decision making procedure in accordance to their misbehavior of nodes. Finally this model demonstrates the effective dealing with misbehavior nodes.

B. F3TM: Flooding Factor based Trust Management Framework

This work was presented by Malik N. Ahmed, Abdul Hanan Abdullah [30]. This work proposes flooding factor based framework for Trust management (F3TM) in MANET. The attacker nodes are identified by calculating the trust value which utilizes true flooding approach. The secure path for forwarding the data is developed by Route Discovery algorithm. The network nodes are validated by Experimental Grey Wolf algorithm. The Optimization of delivery path is identified by Multi-Swarm optimization. They compare the metrics of delay, PDR, overhead and throughput.

C. Bayesian Evidence theorem

This work was presented by Janani V S and Manikandan M S K [31]. This paper presents Bayesian and Evidence theorem and a secured PKI system is designed in the paper that provides the functionality importance of PKI cryptosystem. The efficient method to reduce the insecurity is to feat the mobility character of MANET that converge the trust.

D. Dempster – Shafer Evidence Theory

This work was presented by Bo YANG, Ryo YAMAMOTO [32]. This work proposes a Dempsta –shafer (D-S) evidence based trust management. The proposed method takes control of both black and gray hole attacks. This method observes neighbor model focus on direct trust value to detect single black hole attacks. Evidence of experience node is taken to consider the attacks of gray hole and the neighbor recommendation is combined with indirect trust value to show the cooperative black hole attacks

E. VAST: Volume Adaptive Searching technique

This work was presented by Pragati Dahiya, Rahul Johari [33]. This work proposes Volume Adaptive Searching technique uses to determine the path allocation in a network. VASR algorithm used to minimize the cost and execution time. The proposed VAST algorithm gives the suitable outcome for the adaptation of routing optimization problem.

F. Self-organized key management technique

This work was presented by Saju P John, Philip Samuel [18]. It focuses on the problem related to key exchange. The key exchange is very important in the network for developing the services. This work proposes key management technique that uses key for communication between nodes in a network. This work consists of a server node, cooperative node and other mobile nodes. The cooperative node act as a recommender node between the server node and other mobile node. Each node generated its own key. The key node is certified and validated by using Eigen Vector Reputation centrality.

G. Trust Based Certificate Revocation method

This paper was presented by Banoth Rajkumar, Dr.G.Narsimha [16]. So this paper proposes revocation method, to minimize the attacker nodes and to improve the security. From the direct and indirect trust value the initial trust value is calculated then the secret key is distributed to all nodes. Finally the misbehaving nodes are ignored.

H. Exponential Reliability Coefficient based Reputation Mechanism

This paper as presented by Sengathir.J, Manoharan.R [14]. This selfish behavior will reduce the cooperation among the nodes. An effective mechanism is needed to justify the selfish behavior of nodes. This paper proposes an Exponential Reliability coefficient based Reputation system which separates the narrow minded hub that dependent on Exponential Reliability Coefficient. This dependability coefficient worked through exponential disappointment rate that features the ongoing past conduct of portable hubs for estimating its world.

I. Game theory

This paper was presented by Debjit Das, Koushik Majumder and Anurag Dasgupta [19]. The selfish node will damage the entire communication system. Proposes a Game theory scheme that detect the selfish node and also, by using Least Total Cost Function (LTCF), through least cost path only the data's are transmitted. If a path is broken by a selfish node it automatically selects next best path for data transmission.

J. BoDMaS: Bio-inspired Method

This work was presented by Ahmedin Mohammed Ahmed, Xiangjie Kong [19]. In social network the users are cooperative during the operation of data forwarding. However, selfishness is the misbehavior act of non-cooperation that damages the network performance of social network. This paper proposes BoDMaS, an organically enlivened strategy, that distinguish the issues of narrow-mindedness in an informal community. This work considers a social conduct and microscopic organism's substance item as a counter to accomplish streamlining. Counter is a parameter to investigations the fruitful client including in information activity. This technique surveys and groups clients and neutralizes their self-centeredness. It is assessed from various angles to exhibit its capacity to identify self-centeredness.

K. SENSE: A Collaborative selfish node detection and incentive mechanism

This work was presented by Radu-Ioan Ciobanu,CiprianDobre [22]. The main work of routing algorithm is accepting the data from other nodes under any situations, but this case is not for selfish nodes because these selfish nodes won't accept data from other nodes due to various reasons. i.e., there will be untrusted between the nodes. This work proposes an intensive machine, which punishes the selfish behavior nodes.

L. Selfish replica allocation technique

This work was presented by Byung-Gul Ryu, Jae-Ho Choi [24]. Most of the replication techniques are introduced to reduce the misbehavior of network distribution in MANET. MANET is the self-organized network in which each node has the process of forwarding and receiving the data but the selfishly acting node does not forward the data or it will act partially. So, this paper proposes a selfish replica allocation technique to handle the selfish nodes.

But this approach will take both the selfish behavior and node distance. The selfishness was measured and improves the data accessibility query delay and communication cost.

M. Fuzzy rule based approach

This paper was presented by Mukesh Kumar Garg, Neeta Singh, Poonam Verma [17]. As a result of exceptionally powerful conduct of hubs, it is hard to make sure about a most brief course. Thus, this paper proposes a fluffy guideline based methodology for plan and examination of a Trust–situated in Routing convention. The strength of course is hard to keep up. This proposed calculation is a responsive steering convention which in produced for making a protected course among source and goal. This convention relies upon TV and LOT which chooses the segment activity between the hubs malignant hubs can be handily dispensed with and believed courses are set up.

N. Laplace Stleljes Transform based conditional survivability coefficient model

This work was presented by Sengathir.J, Manoharan.R [13]. Cooperation among the nodes in a network is the important unit for reliable data in a distributed network. But, the selfish nodes will reduce the cooperation and minimizes the network performance. This paper proposes LCSCM that manipulate the accessibility of a node in a network. This method determines the reputation level of a node that quantifies the survivability of a network. 15. Trust management Protocol

This work was presented by Jin-Hee Cho, Ing-Ray Chen [21]. The MANET consists of mixture of nodes may be selfish node. Lack of cooperativeness packet forwarding etc., in existing methods the selfish nodes are detected and isolated. Now the unselfish nodes are encouraged. This paper proposes a trust management protocol for common system where the selfish nodes provide a critical problem in a execution of a system survivability. To encourage unselfish node a tradeoff between each nodes are considered that identifies the best design condition between selfish and unselfish nodes.

O. Trust management Protocol

This work was presented by Jin-Hee Cho, Ananthram Swami [20]. The MANET develops and analyzes a trust management protocol. The trust among mobile node is node suitable for a team collaboration that have new partner but does not have any previous interaction history, this situation is very critical in battlefield. This work identifies the accurate trust level without any risk. Trust metric is defined that provide the unique characteristic of trust chain length and trust level based collaboration in mobile ad hoc network.

P. A novel trust management framework

This work was presented by Wenjuan Fan, Harry Perros [23]. This work addresses the issue of trust the board in cloud condition dependent on appropriated trust specialist co-ops. Outsider, trust specialists are trusted by cloud suppliers, cloud specialist co-ops and cloud administration clients which give trust related administrations to cloud members. Trust specialist organizations are disseminated over the mists and bring out the trust proof from various sources in various arrangements. The information of this evidences are followed by cloud service providers to service level agreement and the feedback is send to cloud service users. Using this information objective trust and subjective trust are evaluated. This proposed work shows the trustworthy of a node in cloud environment.

This work was presented by CHEN Xi, SUN Liang [27]. The busy environment consists of huge number of nodes that communicate in a self-organized network in which the slow moving nodes that does not have the chance to join the network routing. Communication is mainly based on data forwarding operation; there is no need to establish the complete mutual authentication for each conversation. This work proposes a novel trust management scheme based on feedback behavior. The mobile node builds the local certificate graph for the identity trust relationship by the utilization of certificate chain. Behavior trust relationship was generated for slow moving nodes. The result shows the delivery probability and trust reconstruction ratio are improved and it can efficiently explore the trust node for secure data forwarding.

Q. Multidimensional trust based algorithm

This work was presented by Yating Wang, Ing-Ray Chen [25]. In a global wireless technology consists of number of powerful nodes which can provide and receive the services in MANET. The abstracted services are generated by decomposing the requested service and formulate a problem related to optimization that minimize the cost and maximize the QoS. This paper proposes multidimensional trust based algorithm. This algorithm detects the attacks and provides the accurate result to the users, which also achieves the runtime complexity.

R. Trust Management Protocol

This work was presented by Yating Wang, Ing-Ray Chen [26]. This paper proposes a trust management protocol that proves the union properties against attacks. Trust-based algorithm was proposed to solve the problem in optimization requirements. This algorithm has a run-time complexity. It overtakes a non-trust based using blacklists technique that gives the solution to the status node. The analysis result is compared with the design of key parameters and alternative trust protocol. Table-look-up method was developed to detect the dynamically changing environment condition to maximize multi-objective optimization performance.

S. Ant Colony Based DSR

This work was presented by Rajesh Kumar M, Sudhir K.Routray [34]. In a dynamic behavior network, it is very difficult to maintain a secure routing in VANET. The main application of VANET is communication and networking. This work the condition of vehicle according to its metrices. The Ant Colony Optimization is combined with Dynamic Source Routing delivers a high efficient system with better performance.

T. Ant Colony Optimization

This work was presented by Qinghua Shi, Zhong Li [35].Maintaining a secure routing is a major issue in wireless sensor network. For a secure QoS routing, this paper proposes Ant Colony Optimization algorithm. To achieve secure, the credit worthiness of nodes are introduced for ACO algorithm. First the algorithm will eliminate the node which does not satisfy the QoS needs. Then the optimized nodes are send for the ACO algorithm that will prefers the node with credit worthiness and avoid the attackers and also provide high reliable optimized routing. This work was presented by Zhong Luo, Liuzheng Lu [37].

In wireless sensor networks, for maintain a secure data forwarding for Qos, this paper proposes an Trustful Ant Colony routing algorithm. The trust value of the neighbor nodes are calculated for the maintenance of safe data forwarding in an optimized selected path. The result shows the fast and secure data transformation in MANET.

U. ACO-AODV-DHKE Cryptosystem

This work was presented by Sreevidya R C, Nagaraja G S [36]. For consuming energy Ant Colony Optimization (ACO) was proposed and also consumes time during network process. AODV is a multicast routing which transfers a data to destination. Diffie-Hellman Key is used to transfer data in efficient mannar.

V. AODV Protocol

This work was presented by Radha Krishna Bar, Jyotsna Kumar Mandal [38]. Attackers became a problem in MANET. In this work depending on data forwarding of a node is evaluated. AODV routing protocol maintains a path for forwarding the data. By the trust value the nodes are ignored. Thus the data is transferred to a trusted path. The result shows the improved threshold value and less packet drop gives a reliable communication.

This work was presented by Sina Shahabi, Mahdieh Ghazvini [39]. The nodes in Ad hoc network communication and not having any fixed infrastructure or base station. Due to malicious behavior some of the nodes are not supportive to the network. The mentioned attack is black hole attack. The mischievous nodes take the packet and destroy them. So, this work proposes AODV protocol against the attack, it tries to detect the malicious node and ignore from its routing. The result shows in improvement in delay and packet delivery rate.

W. Enhanced-Ant-AODV

This work was presented by Dipika Sarkar, Swagata Choudhury [40]. Optimal path selection is a major issue in MANET. This paper proposes AODV along with ACO for improving Qos in MANET. By ACO with AODV, by a pheromone value the routes are selected for delivering the packets. In proposed work the pheromone value is calculated by end-to-end dependability path, blocking, number of hops and energy. The best routing is chosen according to the highest priority of pheromone value.

X. DSR-ACO

This work was presented by Deepshikha Dhiman, Praveen Sharma [41].Restricted resource and dynamic configuration is the challenging task in MANET. Energy, delay, throughput and jitter are managed to support the Qos. This work concentrated in Qos routing from source to destination. So, this paper proposes Dynamic Source Routing along with Ant Colony Optimization which offers Qos support routing in MANET, also satisfies the parameters like energy, delay, throughput and jitter.

Y. ACO with Global Positioning System

This work was presented by Deepak C. Karia [42]. MANET is a temporary mean of packet delivery between nodes. The source node will transfer the data to terminus node through intermediary nodes. Because of dynamic behavior, finding the optimum route is difficult. So, this paper proposes a biological inspired routing protocol based on ANT along with DSR routing in MANET.

Z. ACO-Enhance DSR

This work was presented by Shubhajeet Chatterjee, Swagatam Das [43]. The dynamic nature of MANET becomes a challenging issue and due to this behavior some of the Qos requirements are not satisfied. So, this paper proposes DSR along with ACO algorithm which produces low delay, energy consumption, etc., First DSR checks the cache for existing routes. Then the initial node delivers the request packet to find the routes. In routing scheme, request ant packet propagates the routing information of nodes in a network to the destination.

Table- I: Comparison of Trusted routing algorithms based on MANET

Sl.No	Author/Ref	Year	Algorithm	Features	Issues	Attackers	Tested Parameters
1.	Janani.V.S [31]	2018	Bayesian-Evience theorem	Trust recommendation and computation reduces the attackers in the network	The mobility of assuming node is not identified	Recommendation, packet dropig, flooding and Sybil attack	Selfishness, time
2.	Mukesh Kumar Garg [17]	2018	Fuzzy rule based approach	Security is maintained in a shortest route	Stability of route is not considered.	Nil	Packet drop, throughput
3.	Malik N.Ahmed [30]	2017	F3TM	The data distribution is secure in MANET. Packet delivery ratio and throughput is high. Delay is lower. Control overhead is lesser.	It does not indicate the presence of attacker node.	Black hole, gray hole, denial-of-service, worm hole,	Delay, Packet delivery ratio, overhead and throughput
4.	Yating Wang [25]	2017	Multidimensional trust based algorithm	Achieves runtime complexity Improves space time complexity in a malicious network.	Trust metrics such as throughput was not achieved.	Self-promoting, Bad-mouthing, ballot-stuffing, Packet dropping attack	Time, throughput
5.	Yating Wang [26]	2017	Trust management Protocol	The trust based solution has low complexity and outperforms the non-trust based solution.	It does not consider the malicious node.	Self-promoting, Bad-mouthing, ballot-stuffing,opportunisticservice attacks	Security, Throughput

6.	Anjali Anand [29]	2016	Partially distributed dynamic model	It improves the secure routing by identifying the misbehavior nodes.	It does not consider the opinion of other nodes while detecting the misbehavior nodes.	Collusion attacks	Observation, experience, recommendation
7.	Banoth Rajkumar [16]	2016	Trust base Revocation Method	Key mechanism is provided to improve the security	Inaccuracy, slow revocation, network overhead.	Nibble attack	Threshold, packet drop, packet delivery ratio
8.	Ahmedin Mohammed Ahmed [19]	2016	BoDMaS	It detects the non-cooperative misbehavior act of selfishness.	Low in transmission speed Does not detect malicious node	Comprising attack	Threshold, Time
9.	Anstar M.Shabut [1]	2015	Recommendation based trust management mechanism	It identify the bogus proposal about a hub in organize	It didn't have any immediate cooperation among hubs	Bad-mouthing, ballot-stuffing and collusion attack	Threshold, packet loss
10.	Saju P John [18]	2015	Self-Organized key management technique	The key exchange is obtained to secure the data flow	No assurance to public key authentication. More time is required to set the trust among each node.	Flooding, Collusion attack	Packet drop, packet delivery ratio
11.	Sengathir. J [14]	2015	Exponential Reliability coefficient based Reputation Mechanism	Lessen the narrow minded hubs by considering the vitality and disappointment rate.	Prediction of mobile node by exponential time is not explored.	Nil	Energy, Selfishness, Throughput, Control overhead, Packet delivery ratio
12.	Debjit Das [15]	2015	Game Theory	Selfish nodes are detected and data is transmitted from source to destination.	Path breaks due to selfish node.	Collusion attack	Selfishness, data cost, Cooperation capability, reputation, dependence
13.	Chen Xi [27]	2015	A novel trust management scheme	It supports forwarding protocols in extremely sparse network	Cannot measure's the reliability of nodes.	Sybil, black hole attack	Data delivery, probability, trust reconstruction ratio
14.	Haojin Zhu [5]	2014	itrust, a probabilistic misbehavior detection scheme	It reduce the detection overhead effectively	Malicious hubs can't be identified after a specific number of rounds.	Black hole or grey hole attackers	Selfishness
15.	Zhexiong Wei [12]	2014	trust management scheme	It obtains the accurate trust value. Throughput and packet delivery ratio is improved.	It does not consider the node which is out of its radio range	Black hole, denial-of-service, worm hole, spoofing an jamming attacks	Connectivity, energy, time
16.	I.R.Chen [7]	2014	dynamic trust management protocol	It improves the trusted secure routing	It doesn't distinguish the childish and pernicious hub outside of its radio range	Self-promoting, Bad-mouthing, ballot-stuffing attacks	Unselfishness, healthiness, Connectivity, energy
17.	Pragati Dahiya [33]	2014	VAST	Adaptive routing optimization is performed.	Connection of nodes in the network changes from time to time.	Nil	Routing ad Computation cost
18.	Radu-loan Ciobanu [22]	2014	SENSE	Selfish nodes are detected and punished	Unnecessary data loss and delay	Nil	Selfishness
19.	Sengathir. J	2014	LCSCM	It detects the selfish node and also calculates the survivability of trusted node.	Based on trust value the packet drop occurs.	Nil	Packet delivery ratio, throughput, control overhead
20.	Wenjuan Fan [23]	2014	A novel trust management framework	Trust worthiness was evaluated in cloud environment	Trust brokers are difficult to predict.	Bad mouthing, on-off, Conflicting misbehavior and newcomer attack.	Qos, Security, Privacy Protection

21.	W.Gao [10]	2013	a novel approach	It accomplishes better execution in sending the information	The information sending is inconceivable inside a brief timeframe	Nil	Data forwarding
22.	Huanyu Zhao [6]	2013	cTrust scheme	It improves the trust relationship in systems	Existing trust doesn't make reference to the issues of versatile hubs	Nil	Threshold
23.	Bo Yag [32]	2013	Dempster-Shafer Evidence Theory	Black and gray hole attacks are detected. Cheating neighbor nodes are detected	The battery power and bandwidth are limited	Black hole and Gray hole attack	Time, Packet rate
24.	Byung- Gul Ryu [24]	2013	Selfish replica allocation technique	Selfish nodes are detected and improves delay, data accessibility and communication cost.	Fully selfish nodes does not hold replica.	Nil	Selfishness, Communication cost, Average Query delay
25.	Jin-Hee Cho [21]	2013	Trust Management Protocol	It analyses the comparison between selfish and unselfish nodes	It does not support in resource – restricted environment	Black hole, Packet dropping attack	Selfishness and altruism
26.	E.Ayday [2]	2012	An Iterative Algorithm	It gives high accessibility of information and proportion of bundle conveyance with low inertness	It doesn't use direct perception based trust getting from interpersonal organization	Byzantine attacks	Data availability, packet delivery ratio
27.	Fenye Bao [4]	2012	Cluster-based hierarchical trust management protocol	It improves the conveyance proportion and message delay without the event of message overhead	Source node does not Forward a packet within a time limit	Forgery, jamming, Sybil, denial-of-service, black hole and slandering attacks	Increase hostility
28.	Ji-Hee Cho [20]	2012	Trust Management Protocol	It provides the accurate trust relation between the mobile nodes by the trust value.	It does not take any previous experience history of a node to calculate the trust value	Denial of Service attack	Energy, Selfishness
29.	Zheng yan [11]	2011	autonomic trust management scheme	It gives powerful answer for the part based framework	It does not consider direct trust	Malicious misbehaviour and common attacks	Healthiness
30.	Pedro B.Velloso [ ]	2010	Scalable Maturity-Based Model	It reduce the number of message	It doesn't appropriate the trust data over the whole system	Sybil, slander and collusion attacks	Energy
31.	Rajesh Kumar M [31]	2016	Ant Colony Optimization, Dynamic Source Routing	It give profoundly effective framework better deferral and parcel conveyance proportion	Difficult to maintain a secure routing	Nil	Delay, Throughput, Energy, Delay jitter
32.	Qinghua shi [32]	2013	Ant Colony Optimization	Secure routing in maintained and attaackers are identified	Nodes does not satisfy the Qos needs	Worm hole, sink hole, flooding, sybil	Delay
33.	Sreevidya R.C [33]	2018	ACO-AODV-DHKE Cryptosystem	Maintain secure routing and also consumes the processing time	Does not maintain permanent route table	Nil	Delay, Packet delivery ratio, Packet loss, energy, security and throughput
34.	Zhong Luo [34]	2015	Ant Colony Optimization	Routing is fast, secure and energy efficient	Due to week energy all packets are not send to destination	Nil	Time delay, bandwidth and energy
35.	Radha Krishna Bar [35]	2013	AODV Protocol	It gives higher threshold value and less packet drop which provide reliable communication	It is difficult to detect a black hole attack	Black hole	Packet drop, Packet loss
36.	Sina Shahabi [36]	2015	AODV Protocol	Malicious nodes are detected and ignored from routing	Some nodes are not supportive to the network	Black hole	Delay, Packet delivery ratio
37.	Dipika Sarkar [37]	2018	Enhanced-Ant-AODV	Optimal path is selected for routing	Not good for real time audio and video transmission	Nil	End-to-end reliability, congestion, number of hops, energy
38.	Deepshikha Dhiman [41]	2016	DSR-ACO	It generates much better throughput with low delay varience	It does not interchange routing information	Nil	Energy, delay, throughput, jitter

39.	Deepak C. Karia [42]	2013	ACO with Global Positioning System	Quickly fins the optimum route	Delay is not tolerant in some application.	Nil	delay, throughput, packet delivery ratio and route cost
40.	Shubhajeet Chatterjee [43]	2015	ACO-Enhance DSR	Efficient routing is performed by avoiding congestion and link breakage	It cannot ensure end-to-end path reliability due to intermediate link breakage.	Nil	delay, low routing overhead, low energy consumption, packet delivery ratio.

III. DISCUSSION OF ALGORITHMS

In Mobile Ad hoc arrange the hubs are influenced by the egotistical malevolent assaults that influence the protected directing in system and it was unraveled by utilizing a portion of the location component and improves the proficiency of the steering by recognizing the perniciousness in a system. The malicious node mainly affects the trust relation between the nodes.

The nodes which are outside of its range use a recommender node. The trust value should be calculated for the recommender node. Some of the existing work does not consider the node which is out of its radio range and does not have any direct interaction among nodes.

For this recommendation based trust management scheme [1, 10, 12] was used, so that the accurate trust value was obtained so that the selfish malicious nodes are detected and improves the throughput and packet delivery ratio and also it detect the false recommendation about a node in a network. The MANET is a distributed network in this the nodes are randomly distributed in a network, the nodes will change its location from time to time, so it is very difficult to calculate the trust value and also to predict the maliciousness in a node. Some nodes does not support in resource- restricted environment. Due to the movement of noes the recommender node will calculate the trust value by the previous history of a node.

But I some network it does not allow to take the previous experience history information to calculate the trust value, so for this trust management protocol [20, 21] was used to provide the accurate trust relation between the mobile nodes by the trust value and also it analyses the comparison of selfish and unselfish node.

In some case, the nodes in MANET are affected by the selfish malicious attacks that affect the secure routing in network that was solved by detection mechanism to improve the efficiency of routing ie., Trust based algorithm [5, 29, 30], that accomplishes the course time multifaceted nature and space time unpredictability in malignant system.

Some system influence the reliability of a hub because of the malignant hub conduct [2] based o notoriety the executives. In some system the source hub doesn't advance a parcel inside a period cutoff and it was illuminated by various leveled trust the executives [4] that improves conveyance proportion and message delay without the event of message overhead. It doesn't disperse the trust data over the whole system [8] that lessens the ability of message and disseminates the trust connection.

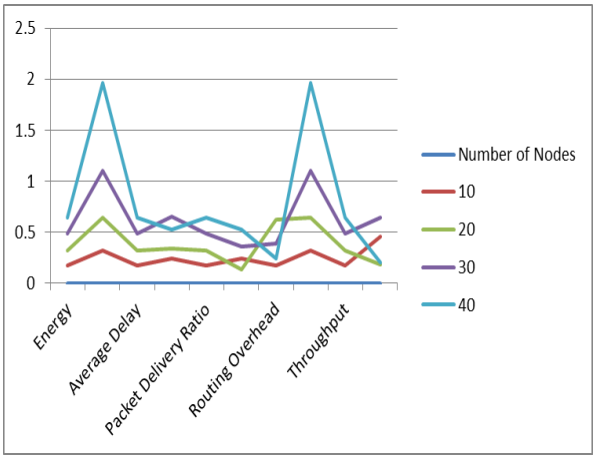

Figure 1: Analysis of paremetres in trusted MANET

The above figure shows the overall analysis of the trust management in Mobile Ad hoc Network. By the evaluation of certain parameters such as Energy, Average Delay, Packet Delivery Ratio, Routing Overhead, Throughput, the trust between the nodes are verified.

Secure data distribution is a difficult task in Mobile Ad hoc Network environment. In traditional routing methods for MANETs, Hybrid Trust Model (HTM) was proposed in MANETs; here advancement strategy is utilized that is Ant Colony Optimization (ACO) [32, 35]. This ACO calculation finds the briefest way from source hub to neighbor hub. ACO calculation gives key to every single hub. By giving key [33, 37] to every hub, the hubs are safely kept up. The key age likewise assists with maintaining a strategic distance from the information duplication, information drop, and so on. The ACO calculation will send the information individually so it will take some multiple occasions to convey the information. So as to control the time, DSR directing convention [35, 37] was utilized. DSR keeps up channel and door. First the hubs will send the information to the channel. The channel will check whether the hubs are approved are most certainly not. On the off chance that it is approved the hubs send the information through the portal, so the time is additionally devoured and the information is likewise safely kept up.

The comparison of the relate work is given in Table 1. The current system doesn't yield noteworthy execution picks up I secure steering among the egotistical vindictive hubs [9, 2, 6, 15, 18]. The present perspective on the trust the board for organize security was first disconnected with approach producer, a conveyed trust the executives structure previously inspected in to the trust the executives issue moving the ides of trust security away from outsider. The trust of a hub is influenced by narrow minded and vindictive hubs in MANET [3]. Here the hub will send the parcel to the goal through the transitional hub in an agreeable way. So the forecast of trust in moderate hub is troublesome.

By estimating a portion of the parameters like availability, vitality, unselfishness the trust can be anticipated in a hub. This paper overviews diverse trust based conventions which gets the trusted steering in childish and noxious influenced hubs in a system.

IV. CONCLUSION

Trust and trust the board are the dynamic research territory in this day and age. Right now overviews about different endeavors made to upgrade execution of overseeing trust in narrow minded and noxious influenced hub in MANET. The hubs in MANET are disseminated in way along these lines, it doesn't have any fixed topology and the assurance of narrow minded and noxious hub is troublesome. By the usage of a portion of the trust related calculation the egotistical hubs are identified and improve the effectiveness of the system.

The above talked about writing gives answer for issues in hub by dissecting different calculations. The issues investigated from our overview can be overwhelmed by the presentation of secure steering in MANET.

REFERENCES

1. Antesar M. Shabut, Keshav P. Dahal, Sanat Kumar Bista, and Irfan U. Awan, "Recommendation Based Trust Model with an Effective Defence Scheme for MANETs",*IEEE Trans On Mobile Computing*, Vol. 14, No. 10, Oct 2015.
2. E. Ayday, H. Lee, and F. Fekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay Tolerant Networks," *IEEE Transactions on Mobile Computing*, DOI: 10.1109/TMC.2011.160, online avaiable, 2011.
3. E. Bulut, Z. Wang, and B. Szymanski, "Cost Effective Multi-Period Spraying for Routing in Delay Tolerant Networks," *IEEE/ACM Transactions on Networking*, Vol. 18, No. 5, 2010, pp. 1530-1543.
4. F. Bao, I.R. Chen, M. Chang, J.H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection", *IEEE Trans. Netw. Serv. Manage*, Vol.9, No.2, pp. 161–183, June 2012.
5. H. Zhu, S. Du, Z. Gao, M. Dong, Z. Cao, "A probabilistic misbehavior detection scheme towards efficient trust establishment in delaytolerant networks", *IEEE Trans. Parallel Distrib. Syst*, Vol. 25, No. 1, Jan 2014.
6. Huanyu Zhao, Xin Yang, and Xiaolin Li,"cTrust: Trust Management in Cyclic Mobile Ad Hoc Networks*", IEEE Trans On Vehicular Technology*, Vol. 62, No. 6, July 2013.
7. I.R. Chen, F. Bao, M. Chang, J.H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing", *IEEE Trans. Parallel Distrib. Syst*. Vol. 25, No. 5, May 2014.
8. P.B. Velloso, R.P. Laufer, D. de O Cunha, O.C. Duarte, G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model", *IEEE Trans. Netw. Serv. Manage*, Vol. 7, No. 3, pp. 172–185, Sep 2010.
9. Yi Ren, Vladimir I and Frank Y. Li, "A Novel Approach to Trust Management in Unattended Wireless Sensor Networks", *IEEE Trans On Mobile Computing*, Vol. 13, No. 7, July 2014.
10. W. Gao, G. Cao, T.F. La Porta, J. Han, "On exploiting transient social contact patterns for data forwarding in delay-tolerant networks", *IEEE Trans. Mob. Comput*., Vol.12, No.1, pp.151–165, Jan 2013.
11. Zheng Yan, and Christian Prehofer, "Autonomic Trust Management for a Component-Based Software System", *IEEE Trans On Dependable And Secure Computing*, Vol. 8, No. 6, Nov 2011.
12. Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning" ,*IEEE Trans on Vehicular Technology*, Vol. 63, No. 9, Nov 2014.
13. J. Sengathir, R. Manoharan, "Laplace Stleltjes Transform based Conditional Survivability Coefficient Model for mitigating Selfish Nodes in MANETs", *Egyptian Informatics Journal* , Vol.15, pp.149–157, Aug 2014.
14. J. Sengathir , R. Manoharan "Exponential Reliability Coefficient based Reputation Mechanism for isolating selfish nodes in MANETs", *Egyptian Informatics Journal* , Vol.16, pp.231–241, July 2015.
15. Debjit Das, Koushik Majumder, and Anurag Dasgupta, "Selfish Node Detection and Low Cost Data Transmission in MANET using Game Theory", *Procedia Computer Science*, Vol.54, pp. 92-101, 2015.
16. Banoth Rajkumar, Dr.G.Narsimha, "Trust Based Certificate Revocation for Secure Routing in MANET", *2nd International Conference on Intelligent Computing, Communication & Convergence*, Vol.92, pp.431-441, 2016.
17. Mukesh Kumar Garg, Neeta Singh, Poonam Verma, "Fuzzy rule-based approach for design and analysis of a Trust-based Secure Routing Protocol for MANETs",*International Conference on Computational Intelligence and Data Science*, Vol.132, pp.653-658, 2018.
18. Saju P John , Philip Samuel, "Self-organized key management with trusted certificate exchange in MANET",*Ain Shams Engineering Journal* Vol.6, pp.161–170, Mar 2015.
19. Ahmedin Mohammed Ahmed, Xiangjie Kong , Li Liu , Feng Xia, Saeid Abolfazli , Zohreh Sanaei , Amr Tolba, " BoDMaS: Bio-inspired Selfishness Detection and Mitigation in Data Management for Ad-hoc Social Networks", *Ad Hoc Network*s, Vol.55, pp. 119–131, Feb 2017.
20. Jin-Hee Cho, AnanthramSwami , Ing-RayChen ," Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks", *Journal of Network and Computer Applications*, Vol.35, pp. 1001–1012, May 2012.
21. Jin-Hee Cho, Ing-Ray Chen,"On the tradeoff between altruism and selfishness in MANET trust management", *Ad Hoc Networks*, Vol.11, pp.2217-2234, Nov 2013.
22. Radu-Ioan Ciobanu,CiprianDobre , MihaiDascălu, ȘtefanTrăușan-Matu, ValentinCristea, "SENSE: A collaborative selfish node detection and incentive mechanism for opportunistic networks", *Journal ofNetwork and Computer Applications*, Vol 41, pp.240-249, May 2014.
23. Wenjuan Fan, Harry Perros, "A novel trust management framework for multi-cloud environments based on trust service providers", *Knowledge-Based Systems* ,Vol .70, pp.392-406, Nov 2016.
24. Byung-Gul Ryu, Jae-Ho Choi, SangKeun Lee, "Impact of node distance on selfish replica allocation in a mobile ad-hoc network", *Ad Hoc Networks*, Vol. 11, pp. 2187-2202, Nov 2013.
25. Yating Wang, Ing-Ray Chen, Jin-Hee Cho, Ananthram Swami and Kevin S. Chan, " Trust-based Service Composition and Binding with Multiple Objective Optimization in Service- Oriented Mobile Ad Hoc Networks", IEEE Transactions on *Services* Computing, Vol 10, pp.660-670, 2017.
26. Yating Wang, Ing-Ray Chen, Jin-Hee Cho, and Jeffrey J.P. Tsai, " Trust-Based Task Assignment with Multi-Objective Optimization in Service-Oriented Ad Hoc Networks", IEEE Transactions on *Network* and *Service* Management, Vol.14, pp.217-232, 2017.
27. CHEN Xi1,3, SUN Liang2, MA JianFeng 3, MA Zhuo, "A Trust Management Scheme Based on Behavior Feedback for Opportunistic Networks", *Network Technology and Application*, pp.117-129, April 2015.
28. Zheng Yan, Pu Wang, Wei Feng, **"**A Novel Scheme of Anonymous Authentication on Trust in Pervasive Social Networking**",** *Information Sciences,*2018.
29. AnjaliAnand; HimanshuAggarwal; RinkleRani,"Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks", *IEEE Journal of Communications and Networks*, Vol.18, pp.938-947, 2016.
30. Malik N. Ahmed, Abdul Hanan Abdullah, Hassan Chizari, Omprakash Kaiwartya, "F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs", *Computer and Information Sciences*, Vol 29, pp. 269–280, 2017.
31. Janani V S and Manikandan M S K, "Efficient trust management with Bayesian- Evidence theorem to secure public key infrastructure-based mobile ad hoc networks", *EURASIP Journal on Wireless Communications and Networking*, Feb 2018.
32. Bo Yang, Ryo Yamamoto, Yoshiaki Tanaka, "Dempster-Shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs", 16th IEEE International Conference on Advanced Communication Technology, pp.223-232, 2014.
33. Pragati Dahiya; Rahul Johari, "VAST: Volume adaptive searching technique for optimized routing in mobile ad-hoc networks", IEEE International Advance Computing Conference (IACC), pp.1-6, 2014.

34. Rajesh Kumar M, Sudhir K.Routray, "Ant Colony Based Dynamic Source Routing For VANET", *International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, pp. 279 – 282, 2016.
35. Qinghua Shi, Zhong Li, "A Secure QoS Routing Algorithm Based on ACO for Wireless Sensor Network*" IEEE International Conference on High Performance Computing and Communications*, pp.1241 – 1245, 2013.
36. Sreevidya R C, Nagaraja G S, "Secure Multicast Routing for Wireless Sensor Networks using ACO-AODV with DHKE Cryptosystem*", International Conference on Computing Methodologies and Communication (ICCMC)*,pp. 733 – 737, 2018.
37. Zhong Luo, Liuzheng Lu, "An Ant Colony Optimization-based Trustful Routing Algorithm for Wireless Sensor Networks" *International Conference on Computer Science and Network Technology (ICCSNT)*, pp.1128-1131, 2015.
38. Radha Krishna Bar, Jyotsna Kumar Mandal, "QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack" *International Conference on Computational Intelligence: Modeling Techniques and Applications CIMTA)*, pp. 530 – 537, 2013.
39. Sina Shahabi, Mahdieh Ghazvini, "A modified algorithm to improve security and performance of AODV protocol against black hole attack" *Wireless Netorks*, Vol 22, pp 1505–1511, July 2016.
40. Dipika Sarkar, Swagata Choudhury, "Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network" *Journal of King Saud University – Computer and Information Sciences*, 2018.
41. Deepshikha Dhiman, Praveen Sharma, "Dynamic Source Routing Protocol Using Ant Colony Optimization Mobile Ad Hoc Networks" *International Journal of Science, Engineering and Technology Research (IJSETR)*, Vol 5, Issue 6, June 2016.
42. Deepak C. Karia ; Vaibhav V. Godbole, "New approach for routing in mobile ad-hoc networks based on ant colony optimisation with global positioning system" *IET Journals & Magazines*, Vol 2, pp 171 – 180, 2013.
43. Shubhajeet Chatterjee, Swagatam Das, "Ant colony optimization based enhanced dynamic source routing algorithm for mobile Ad-hoc network" Information Sciences, Vol 295, pp 67-90, 2015.

AUTHORS PROFILE

Ms. M.Anugraha received the ME Degree in Computer and Engineering from Noorul Islam University, Kumaracoil. Presently she is working as Assistant Professor at Annai Velankanni College of Engineering, Kanyakumari, Tamilnadu. Also she is a Research Scholar at Noorul Islam University. Her research interests include Trusted data transmission in Mobile Adhoc Network.

Dr.S.H. Krishna Veni received her M.E. Computer Science and Engineering from Anna University and Ph.D. Computer Science and Engineering M.S. University. Presently she is working as Associate professor in CSE department of Baselios Mathews II College of Engineering , Kollam, Kerala. She has 15years of diverse experience in teaching, Life member of ISTE, and IEEE Member. Her Research interests in Image processing, network Security , Data Mining and Soft Computing.