DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5075

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

REVIEW PAPER

Available Online at www.ijarcs.info

A REVIEW ON TRUST BASED SECURE ROUTING PROTOCOLS IN AD-HOC NETWORKS

Mr. S. J. Patil
Ph. D. Scholar
Department of Electronics Engineering,
DKTE'S Textile & Engineering Institute, Ichalkaranji.
Maharashtra, India.

Dr. (Mrs.) L.S. Admuthe
Dy-Director
Department of Electronics Engineering,
DKTE'S Textile & Engineering Institute, Ichalkaranji.
Maharashtra, India.

Dr. (Mrs.) M. R. Patil
Principal
JAGM Institute of Technology,
Jamkhandhi, India.

Abstract: A Mobile Ad-Hoc Network (MANET) facilitates communication between nodes whenever & wherever required without any fixed infrastructure. Due to its self-configuring nature, arbitrary topology is formed through wireless links. Such type of Ad-Hoc networks are required at battlefield, rescue operations, during disaster management etc. Although this technology gives a broad range of application in critical conditions, it has its own lacunas. Most importantly, security is the basic issue in this communication mode due to dynamicity of nodes. To ensure secure communication, various types of cryptographic & trust based models have been put forwarded. However, cryptographic methods are not feasible due to intensive computation & low infrastructure network(MANET). Hence trust based models have come in to the existence. The present study includes review on various trust models, with their protocols, advantages & challenges.

Keywords: MANET, Ad-Hoc network, Trust, Routing protocols.

1. INTRODUCTION

1.1 Mobile Ad-hoc Network (MANET)

A mobile Ad-Hoc network is a self-assembled network without any fixed infrastructure. This self-configured network of mobile nodes connected by wireless links to form arbitrary topology. In mobile Ad hoc network, every node act as a router and connection between two nodes is achieved by multi-hop communication. During this communication, nodes in the network can join or leave the network at any instant of time.

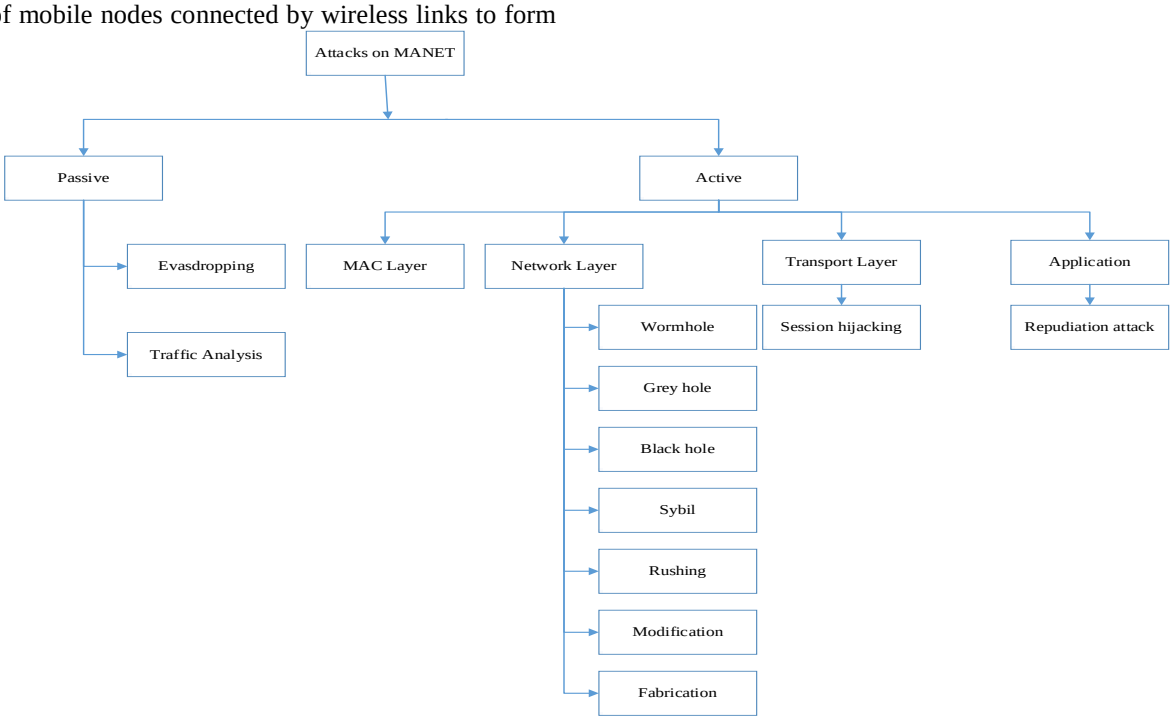

Figure 1. Types of attacks

Due to its dynamic nature, decentralized control, open and shared wireless medium multi-hop communication may lead bandwidth, energy efficiency, memory and lack of cooperativeness are considerable issues with MANET. The susceptibility towards malicious nodes may hamper availability, authenticity, integrity, authorization, privacy and confidentiality.

MANETs might be compromised due to various attacks. They are given in Fig.1

to compromise the security. Along with this, limited resource constraints such as

Passive attack: It is an attack in which the information is snooped without any alteration or disruption.

Active attack: In such type of attack alteration or disruption of information is being made during the exchange of data in the network.

To strengthen MANET various types of security methods have been incorporated in Ad hoc network. These security methods are classified mainly in two groups which are given in Fig. 2

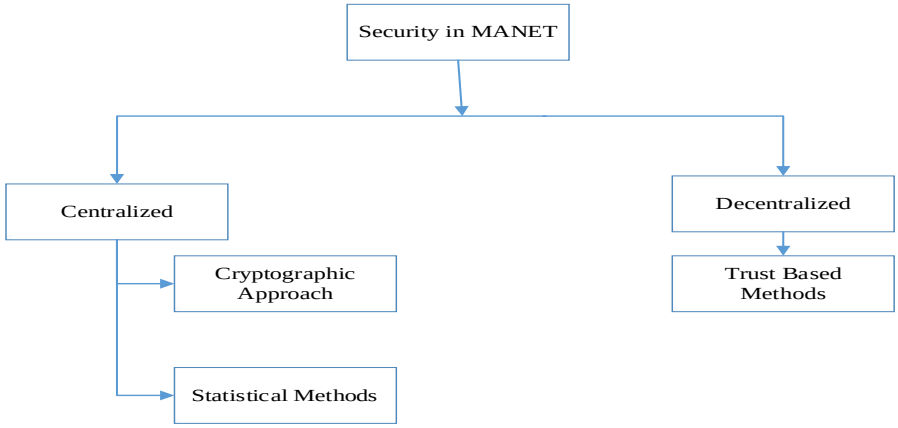

Figure 2. Types of security in MANET.

- **Centralized:**

Centralized model in which trust values are maintained in a common central node or through an authorized third party [1]. However, which goes against the nature of MANET. Centralized models includes cryptographic model and statistical model. The cryptographic approaches provide security through use of symmetric and asymmetric encryption and signature. However, statistical methods are based on statistical properties of links or connectivity information. Cryptographic approaches have their own drawbacks which includes failure to prevent attacks such as wormhole, grey hole, rushing, sybil etc. Along with this, these operations require notable computational and energy overhead due to which this approach is undesirable for small devices.

- **Decentralized:**

In decentralized models each node is assigned by trust and trustworthiness values which are stored and used for future communication. Decentralized approach mainly includes trust based methods. This method is based on natation of trust in network where trust is characterized with the degree of correctness of the behaviour of a network participated in comparison with another.

2. VARIOUS TRUST BASED PROTOCOLS

2.1 Trust Based On-demand Multipath Routing Protocol.

X. Li. et al. [1] Implemented AOTDV routing protocol for MANET. The approach of this protocol includes weighted forwarding ratios to calculate node trust & a path trust as continuous product of node trusts. Forwarding behavior decides whether the node is malicious or not. During discovery of route from source to destination, malicious node may participate but packets might be dropped out so as to calculate trust of such a node, Control Forwarding Ratio can be given less weight than the Data Forwarding Ratio.

2.2 Trust Based AODV (TBAODV):

Mangrulkar & Mohammad [2] proposed trust based AODV (TBAODV), here they added field in RREQ packet which stores trust value indicating node trust on neighbour and the trust factor decides whether to transmit the information or not. The route trust value can be calculated based on reply path and this is utilized by source node for further communication.

The trust value is calculated by product of ratio of nodes individual trust to the average trust, trust of individual neighbour on the route and ratio of hop count average in the route to the individual hop count.

2.3 Trust Modelling & Optimal Routing (TRRP):

Neelkandan & Gokul [3] have proposed trust based optimal routing (TRRP). This paper includes an attack detection & defense mechanism through the route redundancy in Ad-Hoc network. Optimal routing algorithm was developed by the combination of trustworthiness & performance. According to these authors detection of quantitative, difficult, internal attacks & network performance is monitored through the secured routing.

2.4 Association Based DSR (ABDSR):

Bhalaji & Shanmugam [4] have put forwarded dynamic trust based method to mitigate grey hole attack in MANET. In this protocol individual node calculate trust value & association status for all its neighbouring nodes through monitoring their behaviour in the network. Instead of considering only first reception of RREP packet node waits for all neighbouring RREP packets and based on nature of association between them path is decided to be routed.

2.5 Establishment of Dynamic trust among nodes in MANET:

According to researcher [5] along with change in behaviour, trust also changes. This type of dynamic trust is very important because neighbouring node behaviour is not always trustworthy. This protocol is implemented through monitoring of nodes, table maintaining, updating & defining trust for neighbouring node.

In this study the trust T is defined between nodes which is either 1 or 0 and normal behavior is denoted by $t_N = 1$ while malicious behaviour by $t_N = 0$. Whenever node reaches at value 0 will be isolated from the network. This method helps in selecting the optimal & secure path for packet forwarding.

2.6 Multipath Trust based secure AOMDV Routing in Ad-Hoc Networks:

In this research [6] AOMDV routing algorithm hybrided with soft encryption which yielded T-AOMDV. During this, researcher used three steps so as to achieve trust based secure routing, namely message encryption, message routing & message decryption.

In the study message encryption was implemented by using soft-encryption technique where bit operator XOR on a bit vector was used. The message is broken into three parts as a,b &c and encrypted as a'=a XOR c, b'= b XOR c, c'= a XOR b XOR c.

Message routing is achieved by combination of trust mechanism & secure routing process by using node dis-joint AOMDV routing protocol too securely transfer a', b', c'. trust mechanism is computed by

$$Tn = W_d * T_d + W_r * T_r \quad (1)$$

Where, W_d & W_r are some weights assigned to the direct trust value T_d and the trust recommendation T_r, respectively.

The secured routing process was achieved by sending RREQ packet to destination & getting RREP packet back to source. The final step of this protocol is message decryption which involves decryption of a', b' & c' to recover original message through XOR operation which is given as below

a = b' XOR c', b= a' XOR c', c= a' XOR b' XOR c' (2)

2.7 Light weight trust-based routing protocol for mobile Ad-Hoc networks:

In this study authors [7] described light weight trust based routing protocol where intrusion detection system(IDS) was used to estimate the trust which consumes limited computational resource. It also uses only local information by ensuring scalability. Through this protocol authors tried to tackle black hole & Grey hole attacks by using AODV as base routing protocol.

According to this study every node maintains a trust value for each of its neighbours. To account the scalability, the designed trust model so that the trust value is calculated using local information. Ti(j) is the weighted average of two components as given below.

$$Ti(j) = \alpha\ Ti\ (self)(j) + \beta\ Ti\ (neighbour)(j) \quad (3)$$

Where Ti (self)(j) represents the trust of node I on j,
& Ti (neighbour)(j) represents the trust that neighbours of node I has on node j.

Then Ti (neighbour) is given by

$$Ti(neighbour)\ (j) = \frac{1}{n}\sum_{k=1}^{n} Tak(j) \quad (4)$$

In the present protocol route trust value is also considered for secure communication & this route trust value was calculated by following formula

$$Rr = Ta1(a2)\ Ta2(a3)\ldots\ldots Tal\text{-}2(al\text{-}1) \quad (5)$$

$$= \prod_{i=1}^{l-2} Tai\ (a\ i+1)$$

2.8 Trust-Enhanced Message Security Protocol for MANET (ETB-MDSR):

This paper [8] proposed, an enhanced trust based multipath DSR protocol to securely transmit message in MANET's. This protocol consists of a combination of soft encryption, trust management strategy & Multipath DSR routing.

In the first step, message between source & destination node pair is broken in to four message parts and these parts are encrypted by using soft encryption and similar XOR operations. In second step the encrypted message parts transmitted from source to destination by using different trusted multiple paths. In this step a trust management model is implemented where discrete trust levels from -1 to 4 is assigned to each node.

Trust computation is calculated prior to each interaction by considering history of node. Depending on the node history, it is decided that the Tc should be employed for direct computation or indirect computation so as to evaluate the trust values. The level of confidence which decides whether to go for direct computation or indirect computation.

If conf is high then direct trust computation is performed through following equation,

$$T_A(B) = \frac{(ns+1)}{(ns+nu+2)} \quad (6)$$

Where, ns & nu obtained by searching the entries in Ha (B), the history of interactions.

However, conf is low. Then indirect computation is performed through following equation.

$$T_A\ (B) = ns + \sum_{i=1} \frac{ns+1}{ns+nu+\sum_{i=1}(ns)^i+\sum_{j=1}((nu)^j+2)} \quad (7)$$

Where, i is the number of accepted recommendations, $(ns)^k$& $(nu)^k$ are respectively the number of satisfactory & unsatisfactory interaction in the recommendations.

At the destination node, the received encrypted message parts are decrypted using similar X-OR operations.

2.9 TRUNCMAN: Trust based routing mechanism using non co-operative movement in MANET

This protocol [9] is based on AODV with few modifications. Which is divided in two phases namely, Suspicion and detection phase. In suspicion phase as per actual operation of AODV protocol, hello message is used for checking connectivity. Instead of creating neighbour list, it is added into routing table. Once the node broadcast the message to its neighbour, waits for acknowledgement. As it receives acknowledgment back there is confirmation of non-malefic node. If it doesn't receive the reply, there is a assumption of three possibilities for non-cooperative

acknowledgement which include malicious node, low performance node and high traffic node.

In detection phase, when originator doesn't receive the RREQ back in such case either originator will receive reply with delay due to low performance node or with high traffic where there are possibilities for packet being dropped. In such conditions originator will try to communicate neighbour through broadcasting RReq-Ack-Req packet and waits for RReq-Ack-Rep packet. On receiving RReq-Ack-Rep packet, neighbours are considered as non-malicious, while others from which RReq-Ack-Rep packet is not received are considered as malicious node. Against such malicious node non-cooperative packet is broadcasted throughout the network so as to aware the neighbours.

2.10 Requisite trust based routing protocol for MANETs (RTSR)

This work [10] focuses on novel algorithm of trust computation and route detection that detects malicious nodes without message and route redundancy during route discovery RTSR. This protocol is used to detection and defending malicious nodes by using cluster based approach and trust based route discovery through every node in a MANET. By broadcasting the packets route redundancy and message redundancy were reduced. Bandwidth consumption and broadcast storm problem will be reduced by using piggybacking bit.

2.11 A trust based approach for AODV protocol to mitigate black hole attack in MANET

This protocol [11] focuses to mitigate black hole attack. It mainly includes promiscus mode through which neighbours trust value is calculated. This is achieved by following formula

$$T= 1-D/F \quad (8)$$

Where, D is no. of packets dropped by node and F is no. of packets forwarded.

Trust value is in the range of 0 to 1. Initially all neighbouring nodes are given range value of 0.5 by each node whenever trust value is less than threshold; the range value is decremented while if it is more than threshold then it is incremented. Trustworthiness increases with increasing the range value based on this range value below 0.3 were considered as malicious and omitted from communication path.

2.12 HAODV

The present protocol [12] is based on honest mechanism which is calculated by two honest values. Among these, one honest value is based on hop while other is based on trust. Hop dependent honest value might be increased or decreased during RREQ and RREP phase respectively. Calculation of path trust is done by honest value based on trust value.

Before sending data the nodes can evaluate the routing paths according to trusted matrices. This was achieved through,

1. Node creation and authentication
2. Honest value identification
3. Communication and evaluation

Node creation and authentication: In this step, they created a simple pair of nodes to start communication between two nodes. Identity information for each node was created to avoid malicious nodes. Here IP and MAC addresses were used for authentication and initialization.

Honest value initialization: In initialization, two honest values were calculated, where, one is hop based and other is trust based. Hop based value was evaluated by following equation

$$M=P*Q \quad (9)$$

Where, M= Current value of every node

P= Total no. of hops from source to destination

Q= No. of hops from source to current node.

Trust based value was calculated by following equation

N= constant number *Q

Where N= Current trust value of every node

Communication and path evaluation: When source needs to communicate with destination, then it will broadcast RREQ packet. Once destination receives, it will send RREP packet to source. During this phenomenon, hones value based on hop will be decreased while honest value based on trust will remain same in RREQ phase.

In RREP phase, on entry of node at source it verifies with list of neighbor node. In this phase honest value based on hop will be increased by one. Trusted and shortest path was calculated by following formula

$$SP = \frac{Sum of trust values * \sqrt{no. of hops}}{No. of hops} \quad (10)$$

Where, SP= Shortest path

2.13 Distributed trust based routing in MANET

In the proposed work [13] a simple mechanism was adapted which utilize point to point trust matrices derived from various methods. Here, the trust values were used to alter transmission parameter and link layer to reject adversarial paths. The researchers rely on following router protocol and underlying layers.

1. Adversary model
2. Routing model
3. Trust model

The overall trust was computed as a weighted combination of different values with the weights depending on the source of the value.

$$t= w_1t_1 + w_2t_2 + w_3t_3 \quad (11)$$

Where, w_i = Weights of the i^{th} matrices

t1, t2, t3 € [0,1]

During simulation, artificial local congestion was used in untrusted regions to automatically reject paths. It introduces a low overhead in the overall network.

2.14 Trust based security protocol against black hole attacks in opportunistic networks

These are wireless networks which give opportunity to have social interactions and obtain data that can be used for message passing decision. The research [14] encompassed mainly on black hole attack against PROFET routing protocol for opportunistic networks.

In TSP protocol, not only successfully transferred messages decides the trust but also three fundamental pillars like SGV, credits and hop counts involved in it. SGV was given to every individual group with priority number. Each group with different social group value indicates the social importance of groups relative to each other. The trust was calculated by destination node and distributed to each node according to its hop number in the message. To achieve the

distribution of nodes, the destination node of message uses backward path. This feature facilitates quick identification of malicious node. Hence the fact that the node does not participate in routing operation and trust value will never increase.

2.15 Trust based secure on demand routing protocol (TSDRP) for MANET

This work [15] mainly focuses on trust based secure on demand protocol (TSDRP) to tackle black hole and DoS attacks. TSDRP is a modified model of AODV routing protocol which was implemented through node trust table and packet buffer (PB). Information of neighbour's nodes and malicious nodes were stored in node trust table and each node is given node ID. Based on the packet observation, trust value for the node is calculated by following equation,

$$ntv = \max(0, \min(1, c*T_{xyi} + (1-c) * (T_{xyi} + A))) \quad (12)$$

Where, c = constant= 0.93

A = RQC or RPC or DC or BC (13)

= RPC (RREP constant) = 0.3 (success) &

=-0.3 (failure)

RREQ const = 0.3 (success) & =-0.3 (failure)

DC = data constant = 0.4 (success) & =-0.4(failure)

T_{xyi}= Trust of node x on y at i^{th} event = 0.5

BC= black hole constant = - 7.2

PB mainly contains three different types namely PBRREQ, PBRREP and PB Data. These are meant to store control packets and data packets sent by node itself or received from other node and forwarded, based on the algorithm used in promiscuous mode and PB timer.

2.16 Reliable data delivery using trust management system based on node behaviour prediction in MANET

In any communication identification of node behaviour is very important and also provides node recovery scheme. In the present research [16] authors have proposed novel trust management system which is based on node behaviour prediction algorithm. This preserves high network stability and security for reliable data delivery. Prediction and identification of node behaviour is done by this algorithm, through which unintentional temporary errors and intentional malicious behaviour were distinguished and overall trust of node was computed.

Present research consist node behaviour prediction in which various types of node behaviour were predicted such as supportive class, unsupportive class, malicious class and greedy class. Based on this semi-Morkov process was implemented. On the basis of prediction, two measures of a node to evaluate trustworthiness and its recovery process as supportive behaviour prediction (SBP) and malicious behaviour prediction (MBP). This is achieved by cumulative trust computation and trust recovery.

To avoid high overload on network due to the isolation of node, was eliminated through probability model computing PNT using SBP and MBP. It also improves the node isolation rate. The present results give an improvisation in throughput by minimizing network overhead and end to end delay.

2.17 Trusted framework for secured routing in wireless Ad hoc networks.

In the present study [17], both direct (primary) and recommended (secondary) trust opinion was considered to calculate the trust of each node. ARMA/GARCH theory was used in order to compute direct trust of a node. However, proposed trust model also collects recommendation trusts from common neighbours. Finally, the combination of these two will get resulted into weighted combination model.

The study mainly emphases on the mechanism for clustering and cluster head selection which results into calculating node trust and trustworthiness of network. The present work concludes that the proposed trust model performs well with reference to false positive highly congested network. Moreover, the protocol performs its best with CBRP in terms of packet delivery ratio and packet drop rate.

2.18 Trusted secure AOMDV in MANET

The present study [18] includes intrusion detection system and trust based routing which helps in the identification and isolation of attacks. This was carried out in two phase such as route discovery phase and data forwarding phase. Both control packets and data packets which are involved in the route identification and data forwarding phase is secured by IDS.

In the study threshold for routing packet generation rate was measured. In the forwarding phase packet drop of neighbouring nodes were monitored. Finally, direct trust evaluation was done through

$$\text{Source trust} = (\text{RREQ count})^{-1} \quad (14)$$

$$\text{Route trust} = \frac{\text{Forwarded packet count}}{\text{Recieved packet count}}$$

These trust values were stored in trust table.

TS-AOMDV routing process was implemented in two phases namely, trust based route discovery process and trust based data forwarding process.

The study concludes that the present protocol is superior in context to throughput, route selection time, trust non-utilization factor, energy consumption and overhead. This protocol mainly defends grey hole and black hole attacks along with request packet flooding attack.

3. CONCLUSION

Generally, MANET's have a special characteristic but due to its dynamic nature & open infrastructure, security is a key issue. In order to overcome this security, issue various trust based models have been incorporated. In the present review recent security models have been considered so as to analyse their strengths & weaknesses. This review concludes that, models introduced by various researchers have notable disadvantages. Security of any Ad-Hoc network is mainly compromised by various malicious attacks. In this survey, although different models attempted to resolve malicious attacks but all possible attacks have not covered by a single model. Due to nature of Grey hole attack it's difficult to isolate from the network, as it can gain trust before starts dropping packets. Since many of the trust models studied in this review have not particularly considered grey hole attack. Similarly, wormhole attack is also not easy to eliminate from the network.

To prove efficiency of any trust model is based on various parameters such as, PDR, End-to-End delay,

throughput, NRL. Few of protocols have not covered above mentioned parameters. Along with the elimination of malicious nodes without disturbing parameters, energy consumption is a vital issue in MANET. Expect a single model no any other protocol covered energy efficiency module. In consideration to above mentioned aspects, in future an attempt will be made to resolve all drawbacks including energy efficiency & high security.

4. COMPARISON OF VARIOUS TRUST BASED PROTOCOLS

Table1: Comparison of trust based protocols

Authors & Year	Protocol	Attacks considered	Parameters	Advantages	Disadvantages
1. Xin Li. et. al. 2010	AOTDV	Grey hole attack	Packet delivery ratio, End-to-End latency, Path optimality	Finds trusted & shortest path	Colluding attack & efficiency of node is not considered
2. Mangrulkar & Atique 2010	TBAODV	No particular attack is considered	Trust value of node	It improved the trust factor on the neighboring node	Lack of comparative study. Energy of node is not considered
3. Neelkandan & Anand 2011	TRRP	No particular attack is considered	Throughput, Total overhead, Packet delivery ratio & Latency	Combined both trustworthiness & performance	Computational Burdon at each node is not reduced
4. Bhalaji & Shanmugam 2011	ABDSR	Grey hole attack	Packet delivery ratio, Dropped data packet, Route overhead & Throughput	Effective mitigation of Grey hole attack	Broad range of attacks have not considered
5. Saini & Gautam 2011	Dynamic trust model	No particular attack is considered	Node trust	Trust table is maintained at each & every node	Particular parameters are not included & also lack of comparison with other trusted models.
6. Jing et. al. 2011	T-AOMDV	No particular attack is considered	Route selection time, Trust compromise	It requires minimal route selection time	Other parameters are not considered
7. Marchang & Datta 2012	LTB-AODV	Black hole & Grey hole attack	Packet delivery ratio, Malicious packet drop ratio, End-to-End delay, Route frequency, Routing load, Average throughput	Intrusion detection system was used for trust calculation, It consumes limited computational resources & ensured scalability	Increased routing load
8. Woungang et.al. 2012	ETB-MDSR	No particular attack is considered	Route selection time, Total trust compromise	Route selection time & Total trust compromise is reduced against maximum velocity & Malicious node	Not compared with AODV protocol
9. Thanigaivel et. al. 2012	TRUNCMAN	Hidden attack, exposed attack, Pinpoint malicious node	Packet delivery ratio, Data packet dropped	It eliminates non-cooperative node in path discovery phase itself. Considered cognitive network	Primarily considered only PDR & packet dropped
10. Pari et. al. 2012	RTSR	Internal attack, Colluding attack	Throughput, Packet delay, End-to-End delay	Both cluster & trust based approach is used. Colluding nodes are detected, Bandwidth is reduced	Table contents do not matches with graph in respect to end-to-end delay

DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5075

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

REVIEW PAPER

Available Online at www.ijarcs.info

11. Fidel et. al. 2012	Proposed AODV	Black hole attack	Packet delivery ratio	Efficiency of PDR is more in presence of malicious node	Used promiscus mode for trust assignment, trust is based on forwarding behavior
12. Gupta & Pandey	HAODV	External & DoS attack	Dropped packets, PDR, Throughput	Performance of this model is better with relation to dropped packets & throughput	Packet delivery ratio is less
13. Jain & Baras 2013	Distributed trust based model	No particular attack is considered	Hop count, Non-adversial path delay, Trust	Low overhead in overall network, point -to- point trust matrices	Particular parameters are not considered
14. Gupta et. al. 2013	TSP	Black hole attack	Dropped message, Overhead ratio, Message aborted, Delivery probability	Lower overhead, number of message captured by malicious node is lower, Reduced bandwidth uses	Node delivery probability lowered
15. Aggarwal et. al. 2014	TSDRP	Black hole & DoS attack	PDR, Average throughput, NRL	Protocol is efficient under high traffic & increasing malicious node	Under less malicious node PDF & throughput is less as compared to AODV
16. Pavani & Sathyanarayana 2015	TMS	No particular attack is considered	PDR, Dropped packets, Routing overhead	Semi-markov process is used, It differentiate malicious node & unintentional temporary nodes	Energy efficiency is not considered
17. Alnumay et. al. 2015	Trusted framework	No particular attack is considered	PDR, Packet drop rate	Considered direct & Recommended trust	High rate of computation that requires more energy
18. Arbar & Seyed 2016	TS-AOMDV	Flooding, Black hole, Grey hole attack	Route selection time, Throughput, Trust non-utilization factor, Overhead, Energy consumption	Type of attack is easily captured by IDS	PDR is not considered

5. REFERENCES

1] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, "Trust-based on-demand multipath routing in mobile ad hoc networks," Information Security, IET, vol. 4, issue 4, pp. 212-232, Dec 2010.

2] R. S. Mangrulkar, Dr. Mohammad Atique, "Trust based secured Adhoc on demand distance vector routing protocol for mobile Adhoc network", IEEE, 2010.

3] S. Neelakandan, J. Gokul Anand, "Trust Based Optimal Routing in MANET's", in Proc. IEEE ICETECT, pp. 1150-1156, 2011.

4] N. Bhalaji, A. Shanmugam, "Dynamic Trust Based Method to Mitigate Greyhole Attack in Mobile Adhoc Networks", in Proc. Elsvier Procedia Engineering 30 (2012) pp. 881-888.

5] Radhika Saini, Ravinder Kumar Gautam, "Establishment of Dynamic Trust Among Nodes in Mobile Ad Hoc Networks", in Proc. IEEE, 2011, pp. 346-349.

6] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obidat, Ting-Yun Chi, Sanjay K. Dhurandher, "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks", in Proc. IEEE Globecom 2011.

7] N, Marchang, R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks", IET inf. Secur., 2012, Vol. 6, Iss. 2, pp. 77-83.

8] Issac Woungang, Mohammed S. Obaidat, Sanay K. Dhurandher, Han-Chieh Chao, Chris Liu, "Trust-Enhanced Message Security Protocol for Mobile Ad Hoc Networks", IEEE ICC 2012, pp. 988-992.
9] Thanigaivel G, Ashwin Kumar N, Yogesh P, "TRUNCMAN: Trust based Routing Mechanism Using Non-Cooperative Movement in Mobile Ad-hoc Network", IEEE, pp. 261-266, 2012.
10] S. Neelavathy Pari, B. Narmadhdevi, Sridharan Duraisamy, "Requisite Trust-Based Secure Routing Protocol for MANETs", in Proc. IEEE ICRTIT 2012, pp. 276-281.
11] Fidel Thachil, K C Shet, "A trust based approach for AODV protocol to mitigate black hole attack in MANET", IEEE International Conference on Computing Sciences 2012, pp. 281-285.
12] Naveen K. Gupta, Kavita Pandey, "Trust Based Ad-hoc On Demand Routing Protocol for MANET", IEEE, pp. 225-231, 2013.
13] Shalabh Jain, John S. Baras, "Distributed Trust Based Routing in Mobile Ad-Hoc Networks", IEEE Computer Society 2013, pp. 1801-1807.
14] Sahil Gupta, Isaac Woungang, Sanjay K. Dhurandher, Arun Kumar, "Trust-Based Security Protocol Against Blackhole Attacks in Opportunistic Networks", IEEE, WiMob, 2013, pp. 724-729.
15] Akshai Aggarwal, Savita Gandhi, Nirbhay Chaubey, Keyurbhai A Jani, "Trust Based Secure on Demand Routing Protocol(TSDRP) for MANETs", IEEE, 2014, pp. 432-438.
16] V. L. Pavani, B. Satyanarayana, "A Reliable Data Delivery Using Trust Management System Based on Node Behaviour Predication in MANET", IEEE iCATccT 2015, pp. 280-285.
17] Waleed S. Alnumay, Pushpita Chatterjee, Uttam Ghosh, "A Trusted Framework for secure Routing in Wireless Ad Hoc Networks", IEEE 2015, pp. 190-195.
18] Abrar Omar Alkhamisi, Seyed M Buhari, "Trusted Secure Adhoc On-Demand Multipath Distance Vector Routing in MANET", IEEE Computer Society, 2016, pp. 212-219.

6. AUTHORS BIOGRAPHY

Mr. S. J. Patil - Received the BE degree in Electronics from DKTE's TEI, Ichalkaranji, affiliated to Shivaji University, Kolhapur, and ME degree from same University, currently working as an Assistant Professor in the Department of Electronics, DKTE's TEI, Ichalkaranji, Shivaji University, Kolhapur. He has more than 9 years of teaching experience. He is pursuing Ph.D from VTU, Belgavi in the field of Wireless Networks.

Dr. Mrs. Lalita S Admuthe - Received the M.E. and Ph.D. Degree in electronics engineering from Shivaji University Kolhapur, India in 1994 and 2013 respectively. Since 2013 she has been a Professor in Electronics Engineering at DKTE's Textile and Engineering Institute Ichalkaranji. Currently she is working as Dy-Director and Head of Electronics Engineering Department. Her teaching experience includes the topics of Artificial Neural Networks, Radom Signal Processing, Computer Architecture and Parallel Processing. She has been the adviser of Ph.D. degree dissertation on topics related to Decision making optimization in fuzzy environment and artificial intelligence. Her research interest includes Neural Nets, Fuzzy Logic and Optimization Problems. She is member of IEEE, Computer Society and Life member of ISTE.

Dr. Mrs. Meenakshi R. Patil Graduated in Electronics and communication from PVPIT Budhagaon and received post graduate degree from WCE Sangli in 2002. Completed Ph.D. degree from Shivaji university in 2011. She has published 20 papers in International conferences and 20 papers in International journals. Delivered plenary talk in international conference on audio watermarking. She has worked as session chair in international conference held at RCOE Mumbai. She has attended many Faculty development programs and was also spear for few training programs, involved in organizing national and international conferences, paper presentation contest. Worked as a Jury member for many technical programs. Currently she is working as Principal at Jain AGMIT Jamkhandi.