# The Trust Based Routing Protocols in Mobile Ad Hoc Networks: A Review

Dilraj Singh[1], Amardeep Singh[2]

[1] *Research Scholar, Department of Computer Engineering, Punjabi University, Patiala (email: dilraj@pbi.ac.in)*
[2] *Faculty Member, Department of Computer Engineering, Punjabi University, Patiala*

dilraj@pbi.ac.in

***Abstract*— The security is very vital aspect for implementing MANETs in adverse environment, so research on this aspect has emerged as an important MANET's research area in the recent past. Compared to wired networks, MANETS are more vulnerable to security attacks due to lack of a trusted centralized authority and easy eavesdropping. Various techniques based on cryptography, hash functions and trust etc have been developed. But in this resource scarce and dynamic environment techniques using offline configurations and heavy computation are not suitable. So trust based solutions are viable options, on the basis of review of some trust based techniques we propose a trust based solution for secure routing.**

***Keywords*— Security attacks, Trust, AODV, Packet Delivery Ratio (PDR), Routing overhead.**

## I. INTRODUCTION

In recent years there has been explosive growth of mobile computing devices and their applications in various fields. Wireless networks being one of these, networks can be broadly classified into two categories infrastructure based and infrastructure less networks. The second type of networks is referred as Mobile Ad hoc Networks (MANETs). These mobile nodes can form a network any time without presence of any centralized authority or fixed infrastructure. Due to this dynamic nature the network formed on the fly can be deployed in any situation like battlefields, emergency relief works, on demand conferencing and home networks etc. **[1]**

Another important characteristic of MANETs is the dynamically changing topology which makes security a serious concern. Therefore in order to provide security some mechanism is required, because these networks does not have fixed infrastructure. This is the reason why this task becomes complex. Various techniques have been proposed to secure the networks and data transmission using cryptographic, hash and trust based approaches.

The basic routing protocols for mobile ad hoc networks are based on the assumption that all nodes are benign and do indulge in any malicious activity but this is practically not feasible. In order to have a secure network, an important aspect is a secure route between the communicating nodes, so in this paper we focus on trust based approaches used for secure routing in mobile ad hoc networks. In section 2 various security issues and attacks are discussed, section 3 briefly focus on existing security models, section 4 focuses on concept of trust, section 5 focuses on some trust based routing protocols for network security.

## II. SECURITY ISSUES

Though mobile ad hoc networks have a huge potential in current times but along with the benefits there are certain critical issues related to the security that are also becoming evident. The main security issues for any network can be classified as *authentication*, *authorization*, *non-repudiation*, *integrity*, *confidentiality* **[8],** but in case of ad hoc network another aspect also becomes important i.e. *availability*. So an important challenge emerges to build such a mobile network which allows its users to use its services with security, trust and privacy comprehensively dealt with. The sources of threats can also be classified into two groups **[9].** The first comes from *External* attackers, who try to disrupt the working of the network by injecting erroneous routing information, replacing old routing information or distorting the routing information. The second source of attack which is more severe in nature is caused by the *Internal* nodes which are compromised. These compromised nodes can advertise wrong routing information's. They are quite hard to be traced as they possess all the relevant details regarding the network security and could easily generate valid erroneous information.

### *A. Types of attacks*

Due to these reasons the networks are more susceptible to different types of attacks. In MANETs, the attacks are broadly divided into two categories*; Passive* attacks and *Active* attacks [10]. The passive attacks typically involve eavesdropping of data only. Such attacks are hard to trace. Whereas the active attacks involve actions performed by the adversaries like:

- *Modification based attacks*: Integrity of the packets is basically tampered with Modification attacks. With these attacks, the malicious nodes modify the contents of the packets while forwarding them to achieve a desired outcome.
- *Fabrication based attacks*: When the malicious nodes generate and propagate the false routing messages in the network.
- *Impersonation based attacks*: The Malicious nodes can initiate attacks by masquerading as genuine

node, which is also known as spoofing. When a malicious node acquires the identity of genuine by varying its MAC or IP address with the mala-fide intention of cheat other nodes in the network.

Some of the commonly known attacks in MANETs are *Blackhole Attack*, *Wormhole Attack*, *Rushing Attack*, *Jellyfish Attack*, *Sybil Attack*, *Byzantine Attack*, *Routing Table Overflow*, *Sleep Deprivation*, *Denial Of Service*, *Replay Attack* [3],[4],[5],6],[7].

*I*n order to have a comprehensive security solution from the perspective of complete protocol stack the different layers have different issues, attacks and remedies [2].

Table 1- Layer based issues and attacks

| Layer | Issues | Attacks |
|---|---|---|
| Physical Layer | Signal jamming, denial of service | DoS attack, Jamming, interceptions, eavesdropping. |
| Data Link Layer | Protecting the wireless MAC protocol and providing data link layer security support. | Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness. |
| Network Layer | Protection of ad hoc routing and forwarding protocols. | Wormhole, Blackhole, Replay Routing, table overflow attacks. |
| Transport Layer | Authentication and securing end-to-end communication via encryption/de-encryption techniques | Session hijacking, flooding attack (SYN or ACK) |
| Application Layer | Detecting and preventing viruses, worms, and application abuses | Un-authorized access, Repudiation, data corruption |

## III. EXISTING SECURITY MODELS

As discussed in last section that different layer have their individual issues and concerns so to safe guard the MANETs environment a variety approaches are used. Depending upon type of requirement and threats some of broadly classified techniques that are used are as following:

### *A. Cryptographic based Models*

Security in this approach is provided with the use of cryptographic techniques such as Symmetric or Asymmetric encryption and digital signatures. They are able to successfully provide strong authentication and authorization base along with resistance from non-repudiation and non-malleability of information. But these techniques incur a significant amount of computational and energy overhead which is not desired in MANETs due to resource scarce nodes.

### *B. Distributed Public-Key based Models*

In case of Distributed Public-Key approach the idea is to make use of threshold cryptography to distribute the secret key of the Certification Authority over a number of nodes which are defined as servers. A subgroup of N server nodes out of total nodes joins their partial keys to generate a secret key. This scheme provides a robust solution as the attacker nodes will have to overcome of all the N nodes to gain access to the key after which it can compromise the network security. But this approach requires certain level of pre-configuration which defies the basic charter of the MANETs. In addition to this it consumes considerable amount of resources to keep this process working in a fool-proof manner.

### *C. Distributed Trust based Models*

The Distributed Trust based approach makes use of trust in the same as the human beings use in their day to day activities. As per this approach protocols have mechanisms to calculate, recommend and withdraw trust for participating nodes. Each node has to maintain its database to hold the trust values which are computed from direct or indirect resources. It uses trust categories and trust values to find different levels of trust. This approach though is quite flexible to implement and does not need any offline liaison between nodes which clears support the dynamic nature of MANETs, it has some drawbacks. Like, malicious nodes can collude to ouster a genuine node by propagating false or biased recommendations.

## IV. CONCEPT OF TRUST

As per Diego Gambetta [11] *Trust* can be defined as '*a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of this capacity of ever to be able to monitor it) and in a context in which it affects [our] own actions'.* This concept of trust has its roots in the field of social sciences and is defined as *'the degree of subjective belief about the behaviour of a particular Entity*'. [12]

As we are focusing on the concept of trust from the perspective of MANETs there are certain properties of trust, *Subjective*, *Asymmetric*, *Dynamic*, *Transitive*, *and Context-Dependent*. So Depending upon the properties of the trust illustrated while designing of a trust model the following considerations must be taken into consideration *Decentralization*, *Customizable*, *Non-Cooperative nature*, *Self-Organization*.

A trust model refers to a conceptual abstraction on which to build mechanisms for assigning, updating and using trust levels between the entities in a distributed system [12]. So it can be derived that in given scenario the trust model is a tool which helps the agents in a distributed system to locate reliable peers to perform its tasks. In such a model the important components are:

*Accumulator*: Collecting information about the behaviour if of peer nodes are one of the basic components of trust models.

*Evaluator:* Once the information is collected than it has to evaluated and qualified for the use. Various theories are

available to perform this task like Information Theory, Social Network Theory, Clustering, Cooperative and Non-Cooperative Game theory.

*Action Initiator*: Based on the results of the previous two steps the nodes have to initiate the actions they intend to perform.

## V. EXISTING TRUST BASED WORK

Balakrishan et.al, (2007) proposed a Trust Enhanced security Architecture for MANETs (TEAM), in which a trust model is overlaid on key management, secure routing and co-operation model to enhance network security. In this architecture, the trust worthiness of nodes cannot be biased. As a holistic approach the authors deployed Secure MANET Routing with Trust Intrigue (SMRTI) and fellowship model to achieve the functionality of trust and co-operation models respectively. The SMRTI plays an important role in this architecture by gathering information about the trust of nodes based on direct and indirect sources. Similarly, the fellowship model monitors the behavior of the nodes in the network and passes its feedback to SMRTI. Once a route is shortlisted the key management path comes into picture and secures the packet for the transaction. Based on simulation results it is evident that Packet Delivery Ratio is better than DSR if the malicious behavior of nodes is route modification and packet dropping. The performance is low in case of flooding attack, but it improves over DSR if number of malicious nodes is more than 50%.

Rajaram, A. and Palaniswami, S., (2009) developed a trusted based security protocol which use cross layer approach to achieve confidentiality and authenticity of packets. The proposed protocol is referred as Trust-based Cross Layer Protocol (TCLS). The working of the protocol is divided into 2 phases; the first phase is trust based forwarding. In this phase, each intermediate node adds a hash value of the packets it has forwarded on this route by incrementing it. So when the RREQ reaches the destination node it creates a MAC on a value of Prec (Received Packets) and sends the RREP to reverse route by adding its digital signature. Each intermediate node on reverse path verifies the digital signature of the node forwarding the packet and adds its signature if the node is genuine. At source node when RREP is received it verifies all the signatures of intermediate nodes, it also checks if this packet is received from a node in its neighbour list. In second phase of the protocol, CBC-X (Cipher Block Chaining) mode is implemented at link layer to ensure the security of the packet being transmitted as bit by bit. Based on the simulation the results on NS2 simulator the Packet Delivery Ratio in comparison to other similar protocol LLSP (Link Level Security Protocol) is comparatively good with less delay and overhead even with up to 50% malicious nodes.

Poonam et.al, (2010) proposed a trust based enhancement for base DSR for end to end data security in ad hoc networks. They have modified the traditional route discovery process in two ways; at first every node process the RREQ packet received from different nodes. Secondly they enhance the packets with field to hold trust value. Also the destination node can only respond to the RREQ's. Similarly the RREP packet format is enhanced to hold cumulative trust value from source to destination and vice-versa. Another important feature the authors have incorporated is the time limit allowed for every RREQ packet, if any RREP reply is received before the allowed time frame and if its length is one hop than only it is accepted else it is considered as a RREP from malicious node. Likewise, to provide end to end security they employed soft encryption technique i.e. the different parts of a packet. Based on the simulation results on QUALNET the throughput is much better with increasing number of malicious nodes.

Chatterjee, P. et.al, (2012) have proposed a computationally light weight game theoretic routing protocol Secure Trusted Auction oriented Clustering based Routing Protocol (STACRP), it works on AODV based scheme. According to the proposal, the network is divided into small groups based on their geographical locations and nodes in network are likewise divided into sub-groups member nodes, cluster heads (CH) and guard nodes (GN). In order to choose the CH a voting process is followed. All the route discovery processes are handled via CH which helps in reduction of unwanted traffic in the network and malicious nodes disrupting and alluring genuine nodes. If the trust is high the charges are nominal else with decreasing trust value the charges increase. Based on the simulation results on NS2 simulator the Packet Delivery Ratio is almost same as base AODV, but the routing overhead is very low as compared to base AODV even in case the number of selfishly behaving nodes increases up to 40%.

Thachil, F, and Shet, K.C., (2012) presents an approach based on collaborative trust to mitigate the effect of Blackhole attack for the AODV routing protocol. In this approach every node in the network monitors its neighbours and on basis of this monitoring the trust value is computed. The method adopted caches every packet sent by the node. Then it monitors the transmissions of the neighbours in promiscuous mode to check if they retransmitted the packet. In this way when a node does not participate in the network's working its trust level is reduced below the threshold level and is marked as malicious node. Based on the simulation results in NS2 simulator the packet delivery ratio of the proposed approach is much better than the base AODV protocol. Though with the increase in number of malicious nodes the performance degrades but still this new approach works better.

Thanigaivel, G. et al., (2013) proposed a trust based routing mechanism TRUNCMAN (Trust based Routing mechanism Using Non-Cooperative movement in MANET) which is capable of isolating the non-cooperative nodes during route discovery process and can defend various networks later protocols. Every node after broadcasting the

RREQ packet expects it back; in case of not receiving RREQ back they transmit special kind of packets to check the status with its neighbours. The working of this scheme is divided into 2 phases; suspicion and detection phase. In first phase, if a sending node does not receive back the RREQ packet it becomes suspicious and sends a special packet RReq_Ack_Req message to know about the situation at next node. The receiving node then reverts with an RReq_Ack_Rep to clarify its situation. In case of malicious nodes these special packets are also dropped resulting in detection of non-cooperative node. This scheme is also able to detect the wormhole attack; this is done by checking the nodes existence in routing table. On the basis of simulation results in NS2 the packet delivery ratio of proposed protocol remains better even when more than 40% nodes behave maliciously, in contrast to AODV whose PDR drops considerably.

Eissa et.al, (2013) presents a trust based security scheme for AODV, FrAODV. This proposed friendship based framework uses two algorithms to evaluate the forward (FwEvaluate) and reverse (RvEvaluate) routes. This proposal is also based on an assumption that each node has a unique ID which malicious nodes cannot forge, so this scheme uses IP and MAC address for this purpose. Each node in network maintains a list of friends and assigns a value for this friendship. Any packet from a node not listed in friends list is rejected. Likewise intermediate nodes update the value of friendship and add new routes. Based on the simulation results from NS2 the Packet Delivery Ratio of proposed scheme in presence of malicious nodes is quite high as compared to basic AODV in case of small coverage area irrespective of node speed. In large area its PDR is low than standard AODV at high mobility but at low mobility rate it out performs the AODV. The routing overhead is also reduced in the proposed algorithm as the activities malicious nodes have been contained. Two possible concerns in this approach are offline configurations and an assumption that number of malicious nodes less then benign nodes which are uncertain in real time. With this approach the PDR ratio with low mobility in large coverage areas is quite impressive which means that maliciously behaving nodes are curtailed successfully.

Mohanapriya, M. and Krishnamurthi, I., (2013) in their research paper designed and evaluated a Trust Based Dynamic Source Routing (TBDSR) protocol. Their solution claims to protect transmission in presence of colluding malicious nodes without making nodes to work in promiscuous mode. As per proposal, the nodes monitor the one hop neighbours and other nodes in the network via RREQ packets, as this packet contains the trust information about the nodes. Every intermediate node monitors the path through the RREQ packet and maintains a table to hold the trust value for nodes. In case of doubt the nodes can enquire about the trust value of the nodes using the proposed BHREQ (Black Hole trust Request) and BHREP (Black Hole trust Reply) packets. Based on the simulation results on GlomoSim, the PDR is very high as compared to standard DSR even in presence of about 40% malicious nodes. But with increased security the end to end delay increases in proposed scheme, same stands true for routing overhead.

Table 2- Comparison Trust based Routing Protocols.

| Protocol | Advantage | Disadvantage | Attacks |
|---|---|---|---|
| Balakrishan et. al (TEAM) [13] | Trustworthiness of all nodes of route taken into account | Promiscuous monitoring, use of cryptography & key management | Maliciously & selfishly behaving nodes |
| Rajaram, A. & Palaniswami, S. (TCLS) [14] | Ensured confidentiality & authenticity with use of cross layer security | Offline configuration, trusted path selected over shortest path | Denial of Service attack |
| Gera, P et. al (TMDSR) [15] | Reduces the routing overhead by controlling the broadcast of RREQ | No mechanism to update the trust value and node behaviour | Modification & Packet dropping |
| Chatterjee, P. et. al (STACRP) [16] | Scalable due to Cluster based approach, routing overhead reduced | Promiscuous monitoring and use of cryptography | Sybil, DoS & Flooding attack |
| Thachil, F. & Shet, K.C. [17] | Data transmission monitored so packet dropping attacks prevented successfully | Promiscuous monitoring, as control packets are monitored so malicious can join network easily | Blackhole attack |
| Thanigaivel, G. et. al (TRUNCMAN) [18] | Routing decision are fast as neighbour information available in routing table, this also helps in stopping wormhole attack | Promiscuous monitoring, possible delay added as nodes give second chance to every packet in a fixed frame of time | Maliciously behaving nodes & certain hidden attacks |
| Eissa, T. et.al (FrAODV) [19] | Performs better in large areas | Offline liaisoning, assumption that malicious nodes are less then benign nodes | Malicious nodes |
| Mohanapriya, M & Krishnamurth, I. (TBDSR( [20] | Nodes aware about entire n/w topology, Trust values refreshed periodically | Promiscuous monitoring of entire network, assumption that all nodes are authentic | One & two node based Blackhole attack |

Table 3- Comparison of Packet Delivery Ratio (PDR).

| Malicious Node% / Protocol | 10% | | 20% | | 30% | | 40% | |
|---|---|---|---|---|---|---|---|---|
| | Prpsd | Base | Prpsd | Base | Prpsd | Base | Prpsd | Base |
| TCLS | 78% | 70 | 60% | 40% | 58% | 35% | Not considered | |
| TEAM | 63% | 53% | 54% | 40% | 45% | 35% | 38% | 24% |
| TRUNCMAN | 85% | 80% | 65% | 60% | 55% | 48% | 48% | 37% |
| Trusted ADOV | 80% | 5% | 70% | 2% | 55% | 0% | 63% | 0% |
| STACRP | 83% | 78% | 73% | 63% | 75% | 65% | 71% | 61% |
| TBDSR | 90% | 18% | 62% | 30% | 64% | 25% | 60% | 40% |
| TMDSR | 87 | 78% | 86% | 70% | 82% | 68% | 76% | 67% |

Fig 1- Packet Delivery Ratio at 10% malicious nodes

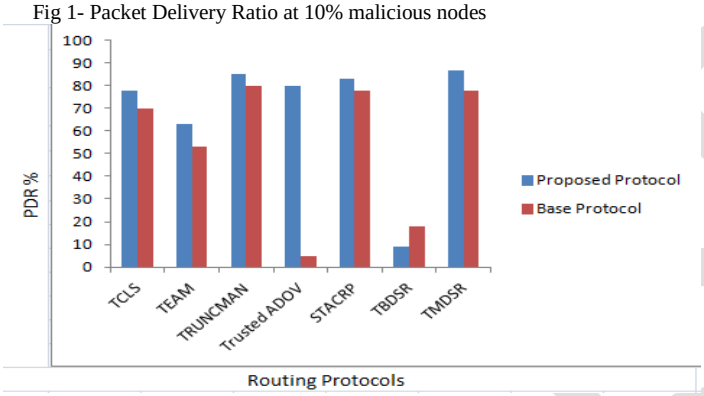



Table 4- Comparison of Routing Overhead.

| Malicious Node% / Protocol | 10% | | 20% | | 30% | | 40% | |
|---|---|---|---|---|---|---|---|---|
| | Prpsd | Base | Prpsd | Base | Prpsd | Base | Prpsd | Base |
| TCLS | 1800 | 1400 | 3600 | 1800 | 4500 | 2200 | Not considered | |
| STACRP | 6400 | 1400 | 5600 | 1400 | 4600 | 1300 | 4000 | 1200 |
| TBDSR | 6100 | 5000 | 5000 | 4100 | 5400 | 5200 | 5800 | 5000 |

Fig 2- Routing overhead at 10% malicious nodes

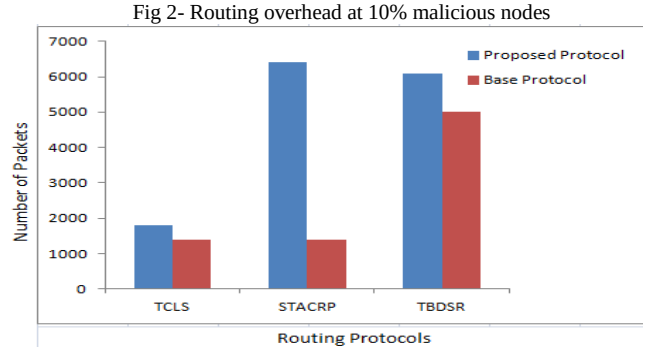
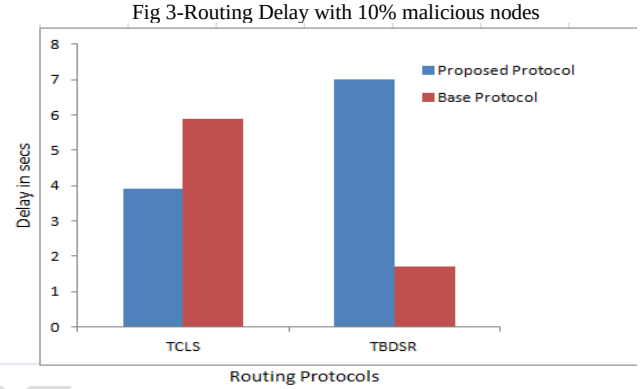



Table 5- Comparison of Routing Delay in seconds.

| Malicious Node% / Protocol | 10% | | 20% | | 30% | | 40% | |
|---|---|---|---|---|---|---|---|---|
| | Prpsd | Base | Prpsd | Base | Prpsd | Base | Prpsd | Base |
| TCLS | 3.9 | 5.9 | 4.5 | 6.2 | 4.6 | 6.5 | Not considered | |
| TBDSR | 7 | 1.7 | 7.5 | 2 | 8 | 2.8 | 7.8 | 2.6 |

Fig 3-Routing Delay with 10% malicious nodes




## VI. Conclusion

The MANETs is one of the emerging areas for research and practical applications, security being one of the critical areas of focus. In this paper we reviewed trust based secure routing protocols; we choose the trust based approach over cryptography and other conventional approaches because of its easy implementation and the limited resource requirements. Based on the review of the approaches proposed by various authors most of them perform quite well in comparison to their compared counterparts. As shown in Table 3 in most cases the PDR of the proposed approaches is above 50% in adverse environments where malicious nodes are up to 40%. But these approaches at same time incur more routing overhead shown in Table 4, likewise routing delay is added as shown in Table 5, because they tend to locate the trusted paths only.

## References

[1] Deng, H., Li, W. and Agrawal, D.P., "Routing Security in Wireless Ad Hoc Networks," IEEE Communications Magazine, pp. 70-75, October 2002.

[2] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., "Security in Mobile Ad Hoc Networks: Challenges And Solutions", IEEE Wireless Communications, pp. 38-47, Feb. 2004.

[3] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N. and Jamalipour, A., " A Survey Of Routing Attacks In Mobile Ad Hoc Networks", IEEE Wireless Communications, pp. 85-91, October 2007.

[4] Gupte, S. and Singhal, M., "Secure routing in mobile wireless ad hoc networks", Elsevier Ad Hoc Networks, pp. 151–174, 2003.

[5] Hashmi, S. and Brooke, J., "Authentication Mechanisms for Mobile Ad Hoc Networks and Resistance to Sybil Attack", Emerging

Security Information, Systems and Technologies, SECURWARE, Cap Esterel, France, pp.120 – 126, 25-31 August 2008.

[6] Jen, S., Laih, C. and Kuo, W., "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", Sensors, pp. 5022-5039, 2009

[7] Johnson, D.B. and Maltz, D.A., "Dynamic Source Routing in Ad Hoc Wireless Networking," Mobile Computing, T. Iemielinski and H. Korth, eds., chapter 5, Kluwer Academic, 1996

[8] Shanthi, N., Ganesan, L. and Ramar, K., "Study of different attacks on Multicast Mobile Ad hoc Network", Journal of Theoretical and Applied Information Technology Vol.10, No.1, pp. 45-51, 2009.

[9] Nyre, A.A., "A survey on security in Mobile Ad Hoc Networks", Security and Communication Networks (IWSCN), 2009 Proceedings of the 1st International Workshop on IEEE, pp.1-6, Publication Year: 2009.

[10] Choi, H., McDanial, P. and Porta, T. F. L., "Privacy Preserving Communications in MANETs", Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07, 4th Annual IEEE Communications Society Conference, pp. 233 – 242, 2007.

[11] Rahman, A. and Hailes, S., "A Distributed Trust Model", Proc. of the ACM New Security Paradigms Workshop, pp. 48-60, 1997.

[12] Cho, J., Swami, A. and Chen, I., "A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, Vol. 13, No. 4, pp. 562-583, Fourth Quarter 2011.

[13] Balakrishnan, V., Varadharajan, V., Tupakula, U. and Lucs, P., "TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks", Networks, Proceedings of the Fifteenth IEEE International Conference on Networks (ICON 2007), Adelaide, Australia, pp. 182-187, 2007.

[14] Rajaram, A. and Palaniswami, S., "A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks", International Journal of Computer Science and Information Security (IJCSIS), Vol 6, No. 1, pp. 165-172, 2009.

[15] Poonam, Garg, K. and Misra, M., "Trust Enhanced Secure Multi-Path DSR Routing", International Journal of Computer Applications, Vol. 2, No.2, pp. 63-69, 2010.

[16] Chatterjee, P., Sengupta, I., Ghosh, S.K., "STACRP: a Secure Trusted AUCTION oriented Clustering based Routing Protocol for MANET", Cluster Computing The Journal of Networks, Software Tools and Applications, 15, pp. 303–320, 2012.

[17] Thachil, F., and Shet, K.C.: "A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET", Proc. International Conference on Computing Sciences, 14-15 Sept 2012, pp.281-285.

[18] 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.

[19] Eissa, T., Razak, S.A., Khokhar, R.H. and Samian, N., "Trust-Based Routing Mechanism in MANET: Design and Implementation", Mobile Networks and Applications, Vol. 18, No. 5, pp. 666-677, October 2013.

[20] Mohanapriya, M. and Krishnamurthi, I., "Trust Based DSR Routing Protocol for Mitigating Cooperative Black Hole Attacks in Ad Hoc Network", Arabian Journal for Science and Engineering, pp. 1825-1833, 2013.