A Survey of Trust Based Routing Protocols in MANETs

Deepika Kukreja, Umang Singh, and B. V. R. Reddy

***Abstract*—A mobile ad-hoc network is a self-configuring network of mobile hosts connected by wireless links which together form an arbitrary topology. Due to lack of centralized control, dynamic network topology and multihop communications, the provision of making routing secure in mobile ad hoc networks is much more challenging than the security in infrastructure based networks. Several protocols for secure routing in ad hoc networks have been proposed in the literature. But due to their limitations, there is a need to make them robust and more secure so that they can go well with the demanding requirements of ad hoc networks. This paper presents a survey of trust based secure routing protocols for mobile ad hoc networks. Different trust based secure routing protocols are discussed and analyzed in the paper along with their strengths, weaknesses and future enhancements.**

***Index Terms*—Routing protocol, trust based secure routing, ad hoc networks.**

I. Introduction

Secure routing protocols is a crucial area towards security of MANET. The routing solutions for conventional networks are not sufficient to work efficiently in ad-hoc environment. Most of the existing work [1]-[8] in the area of secure routing protocols in an ad hoc network is based on key management, heavy encryption techniques or on continuous promiscuous monitoring of the neighbors. These approaches for making ad hoc routing secure are expensive in terms of network bandwidth as they introduce a heavy traffic load to exchange and verify keys, they also consume lots of nodes' energy and come at the cost of computational complexity of encryption techniques thus they do not fit well for MANET. In this paper, we discuss various trust based secure routing schemes.

The rest of the paper is structured as follows: Section II presents an overview of secure routing protocols in ad hoc networks. In Section III, the secure routing protocols based on trust are discussed and analyzed. A comparison of surveyed trust based secure routing protocols is given in Section IV. Section V concludes the paper and discusses several open research issues.

II. Overview of Secure Routing Protocols In Ad Hoc Networks

There are several secure routing protocols in the literature that were designed to cope with the limitations and requirements of ad hoc networks. Marti *et al.* designed Watchdog and Pathrater mechanism [4] to optimize the packet forwarding method in the Dynamic Source Routing (DSR) protocol [9]. It consists of two components: Watchdog and Pathrater. The Watchdog detects selfish nodes that do not forward packets and the Pathrater helps routing protocols to avoid these nodes. It assigns ratings to the nodes, based upon the feedback it receives from the Watchdog. These ratings are then used to select routes having nodes with the highest forwarding rate. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of: Ambiguous collisions, Receiver collisions, Limited transmission power, false misbehavior and Partial dropping.

CONFIDANT (Cooperation of Nodes, Fairness In Dynamic Ad hoc NeTworks) [5] adds a trust manager and a reputation system to the Watchdog and Pathrater mechanism [4]. The trust manager evaluates the events reported by the Watchdog and in order to warn other nodes in the network regarding malicious nodes (for not forwarding), it sends alarm. The reputation system maintains a black-list of nodes at each node and shares this list with the nodes in its friends-list. The confidant protocol is based on a punishment scheme, by not forwarding packets of nodes whose trust level drops below a certain threshold.

Dahill *et al.* proposed Authenticated Routing for Ad-hoc Networks (ARAN) [6] that detects and protects against misbehaviors of malicious nodes in an ad-hoc network. ARAN is based on asymmetric cryptography, make uses of digital certificates and all nodes are supposed to keep fresh certificates with a trusted server and should know the server's public key. ARAN requires the use of a trusted certificate server in the network which is against the nature of MANETs. Y.Hu. et al. proposed SEAD (Secure Efficient Ad hoc Distance vector) [7], based on Destination Sequenced Distance Vector (DSDV) [10] protocol. It uses one way hash function and authentication to differentiate between updates received from malicious and non-malicious nodes. It overcomes the DoS and resource consumption attacks but fails when the attacker uses the same metric and sequence number as used by recent update message. In SEAD nodes have hash chain which has a finite size and must be generated again when all their elements have been used. Y. Hu *et al.* [8] proposed ARIADNE, an on-demand secure routing protocol based on the Dynamic Source Routing (DSR) that protects against node compromise. It is based upon symmetric cryptography and the distribution of shared secret keys between source and the destination. For node authentication ARIADNE prefers using the TESLA [11] broadcast authentication scheme with delayed key disclosure. TESLA requires clock synchronization between communicating nodes and this requirement is unrealistic in MANETs.

Manuscript received May 25, 2013; revised August 1, 2013.

The authors are with University School of Information and Communication Technology, Guru Gobind Singh IndraPrastha University, Delhi, India (e-mail: deepikakukreja@mait.ac.in, singh.umang@rediffmail.com, bvrreddy64@rediffmail.com).

DOI: 10.7763/JACN.2013.V1.56

III. Trust Based Secure Routing Protocols

All the existing work in the area of secure routing in ad hoc networks as discussed in the earlier section is based on key management or heavy encryption techniques or on continuous promiscuous monitoring of the neighbors. These approaches for making ad hoc routing secure are expensive thus they do not fit well for MANET as MANET nodes have limited battery, limited computational capabilities and limited memory for storing security information. In this section we discuss about various trust based secure ad hoc routing schemes.

A. Collaborative Trust-Based Secure Routing against Colluding Malicious Nodes

T. Ghosh *et al.* [12] proposed a trust based AODV (Ad hoc On-Demand Distance Vector) routing protocol shown in fig. 1 that isolates malicious nodes acting independently or in collusion. The protocol requires the existence of a Public Key Infrastructure. As intermediate nodes are not allowed to send RREP, it increases the delay in Route Discovery. In the protocol a method for computing trust can be incorporated.

B. Trust-Embedded AODV (T-AODV)

T. Ghosh et al. [13] proposed Trust-embedded AODV (T-AODV), which extends [12]. The model computes, distributes and updates trust shown in fig. 2 The working of the protocol is same as [12] with a difference that this solution works only when a malicious node sends false accusation. Each node maintains and periodically scans the tables, requiring the nodes to have more memory. The protocol requires existence of a Public Key infrastructure. The solution assumes that all the nodes have identical radio range, which is not realistic in a MANET.

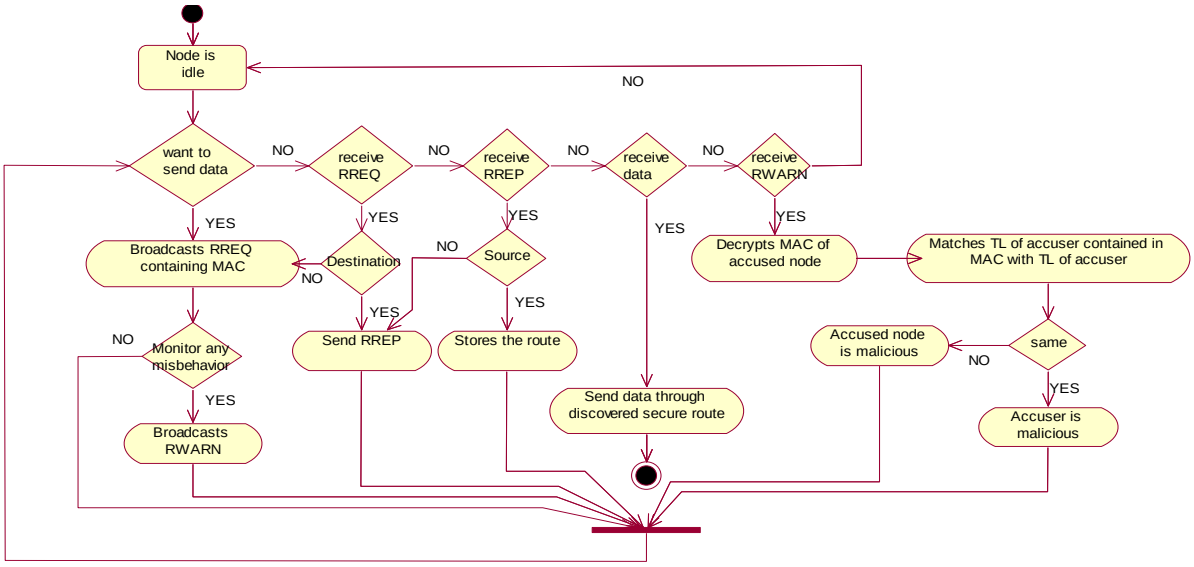

Fig. 1. Process Flow for trust based AODV.

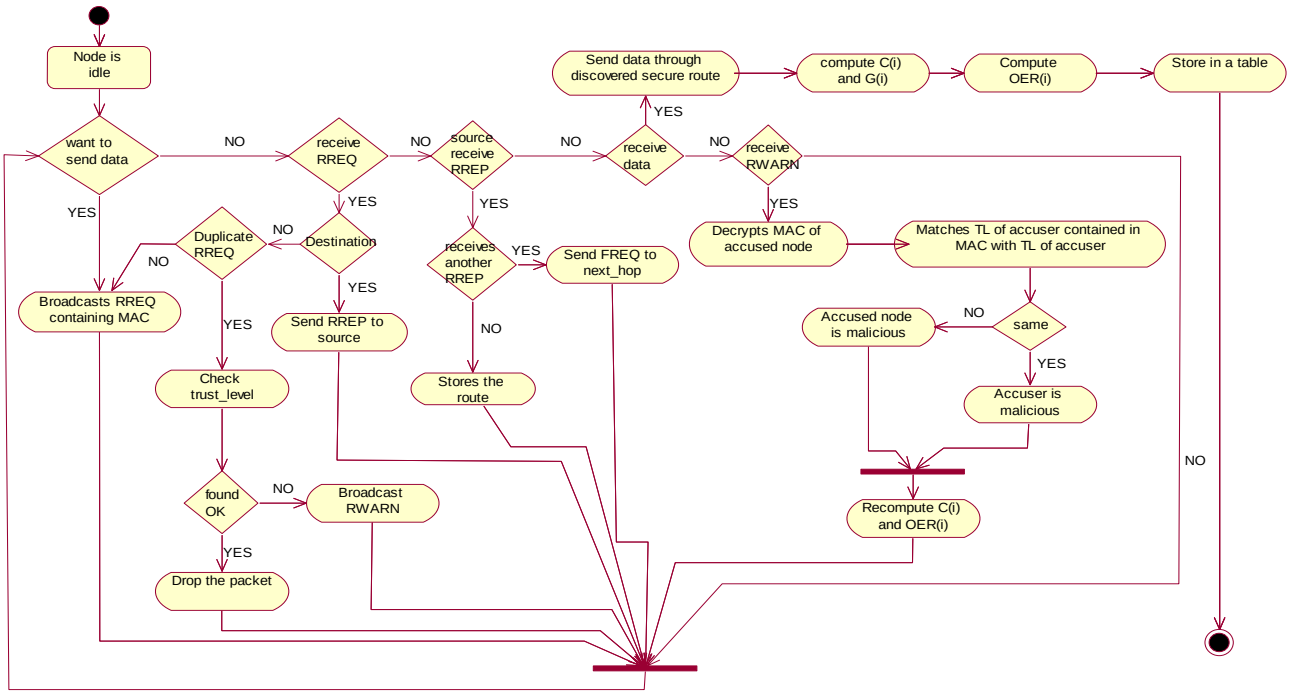

Fig. 2. Process Flow for T-AODV.

C. Trust-Based Routing without Trust Infrastructure

Pirzada et al. [14] proposed a mechanism for establishing trust based routing without the use of a trust infrastructure. Direct trust is based on [4]. When a node transmits a packet, the sending node overhears and verifies the different fields in the forwarded IP packet for modifications.

D. Deploying Trust Gateways to Reinforce Dynamic Source Routing

In [15], authors extended [14] and modified DSR (Dynamic Source Routing) protocol such that intermediary nodes act as Trust Gateways that keeps track of trust levels of the nodes for avoiding malicious nodes. Each node monitors its neighbors and maintains a direct trust value for them. Source node uses this trust information to compute the most trustworthy path. Process flow route selection is shown in fig. 3. The method of computing trust is based only on the forwarding behavior of the nodes. The node executing the Trust Gateway may itself be malicious. The nodes executing the Trust Gateway must have high energy, high computation power, more memory and less mobility.

E. Trust Establishment in Pure Ad-hoc Networks

In [16], a trust-based model based on direct experience is proposed. The model is based on [14] and [15] and uses trust agents that reside on each node. Each trust agent performs three functions: Trust Derivation, Quantification, and Computation. The proposed trust model is applicable for DSR, AODV and TORA (Temporally-Ordered Routing Algorithm). In the proposed model, only direct trust is used for trust computation. As each node selects the most trustworthy next hop, this increases the delay and the resulting returned route may be long. The protocol fails in case malicious nodes collude. Here, direct trust can be combined with indirect trust.

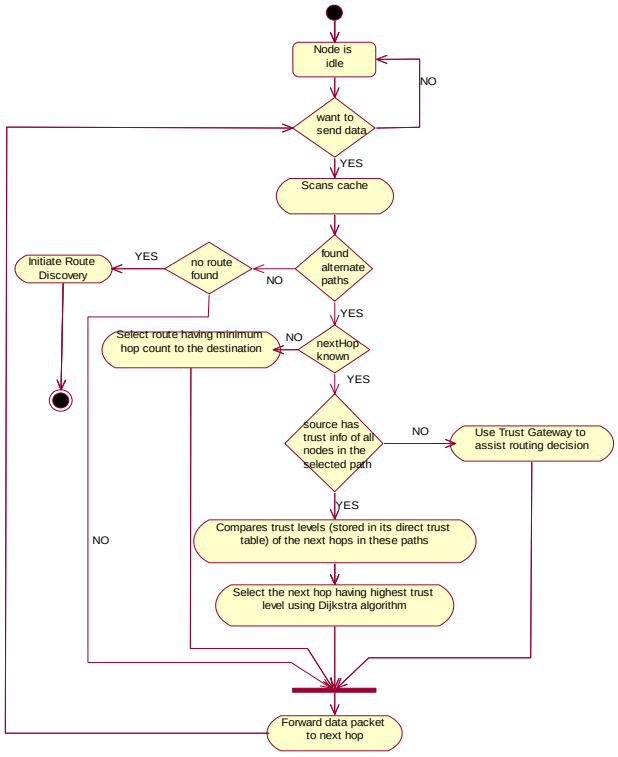

Fig. 3. Process flow for Route selection.

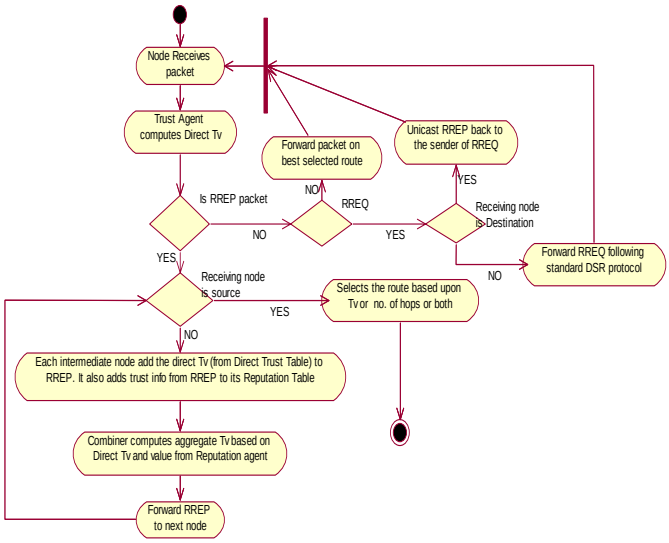

Fig. 4. Process flow for Route selection.

F. Opinion Based Trusted Routing Protocol – TAODV

In [20], TAODV routing protocol is proposed. Trust is represented by opinion as used in subjective logic. If a node behaves in a normal manner, other nodes increase its opinion and otherwise, decrease its opinion as shown in Fig. 6. The nodes authenticate each other by verifying the certificate, which is an added overhead. The protocol is unable to detect an internal attack, in which a malicious node may refuses to forward the packets, authenticates itself to the source but later on acts as a blackhole.

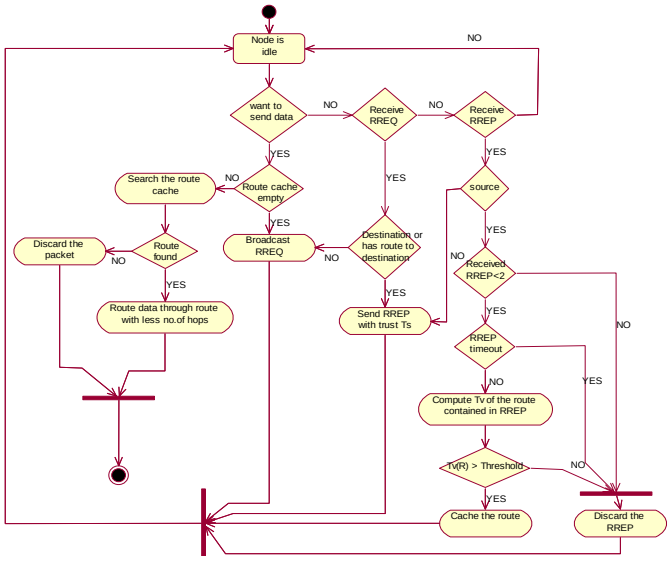

Fig. 5. Process Flow for tr-DSR.

G. Dynamic Mutual Trust Based Routing protocol (DMTR)

A trusted routing protocol called DMTR, based on DSR protocol is proposed [21] that secures the network using the Trust Network Connect (TNC), and improves the path security which is selected by barrel theory. The process flow of the protocol is shown in fig. 7. Exchange of trust table between nodes requires lots of bandwidth as well as increases the overhead.

H. Soft Encryption and Trust-Based Multipath Routing

The proposed paper [22], introduces a method of message

security. It uses soft encryption techniques in which the message is divided into parts and the parts are self- encrypted. The number of encrypted parts of a message given to a node for forwarding depends upon the trust value of that node. This way, a malicious node having very less value of trust cannot access the message. The encrypted message parts of a message are routed through different paths as shown in fig. 8. The proposed method takes more time in route selection and it is not always possible to route all messages securely. The proposed method is further enhanced [23] by taking required security level of the data into consideration.

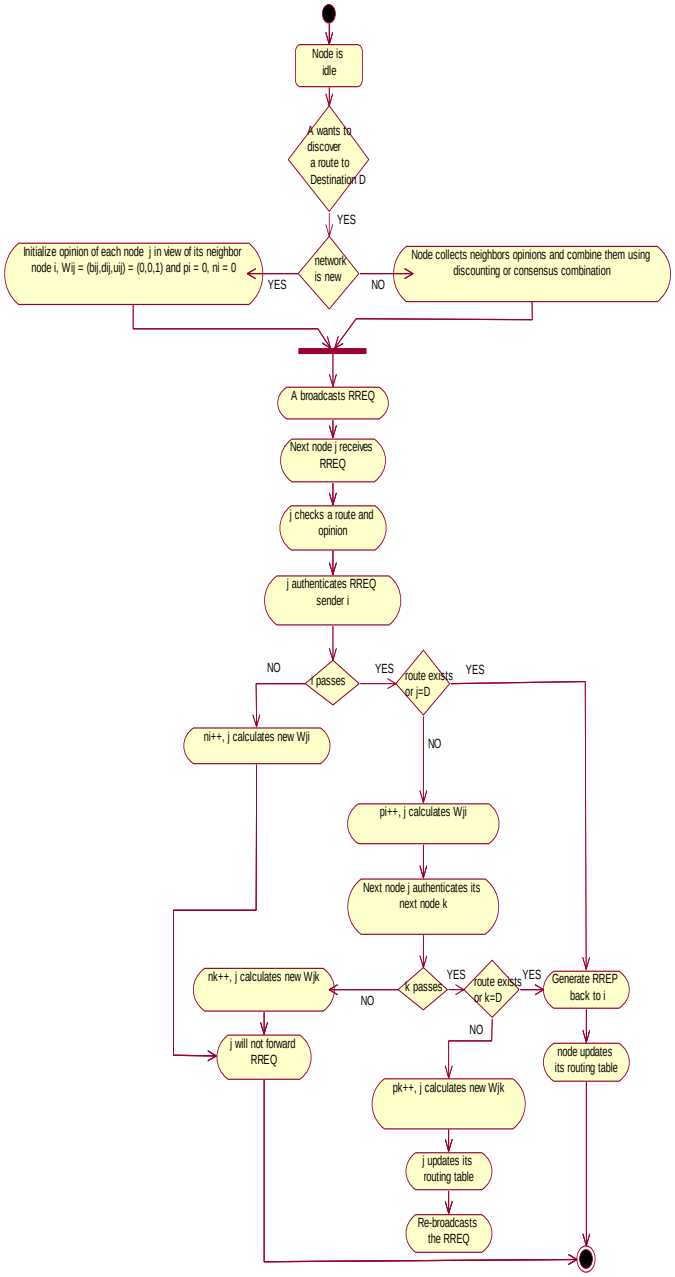

Fig. 6. Process Flow for TAODV.

I. Incorporating Trust and Reputation in the DSR Protocol

A scheme for establishing trustworthy routes has been proposed in [17] as shown in fig. 4. Each node executes the trust model having three main components: Trust agent, Reputation agent and the Combiner. The Trust agent derives the direct trust, the Reputation agent derives the indirect trust and the Combiner computes the final trust by combining the information received from both the agents. If malicious nodes collude the model may fail. If nodes have varying transmission power ranges, the mechanism of passive trust assignment might not work properly. Here, the authors have used five categories for computing direct trust; other categories like for detecting flooding attack, wormhole attack can be included.

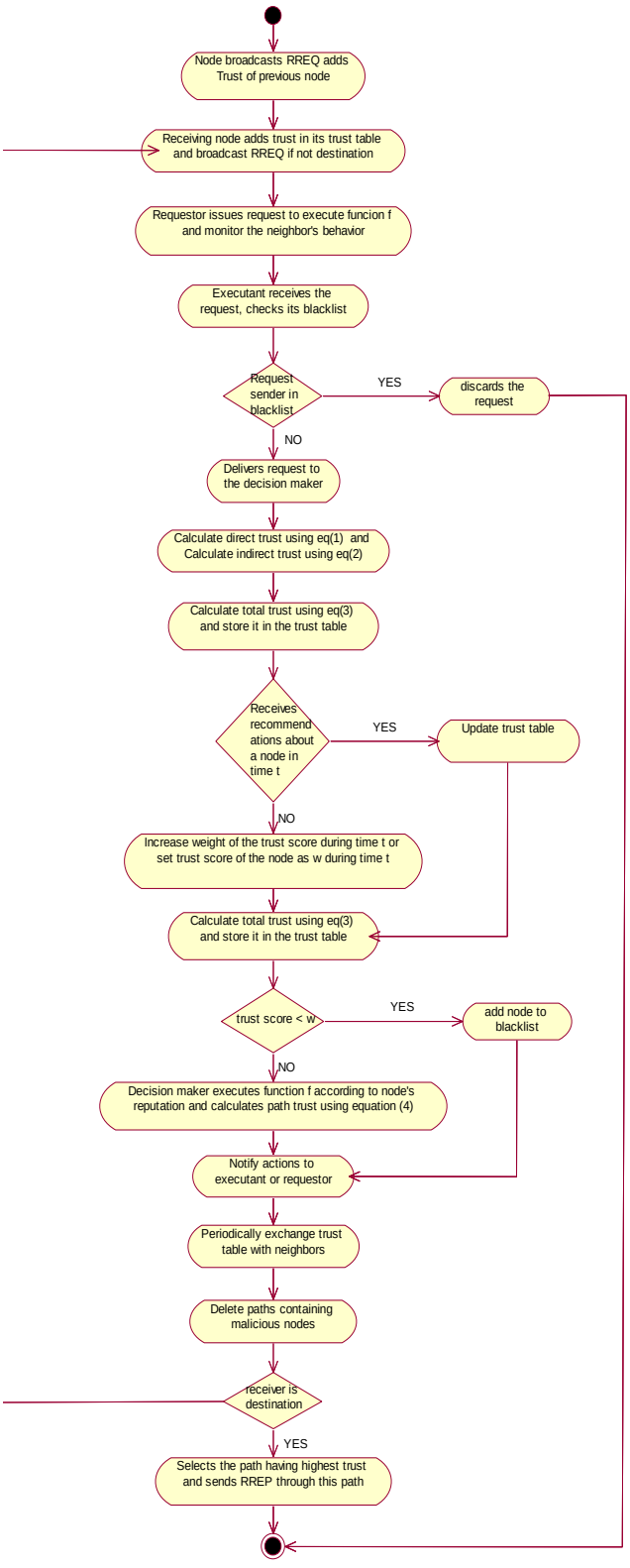

Fig. 7. Process Flow for DMTR.

J. Dependable Dynamic Source Routing Protocol

Pirzada *et al*. [18] presented a trust based DSR routing protocol for discovering routes in the presence of malicious nodes. Each node monitors its neighbors and updates their trust levels depending on their behavior. Trust values are propagated in the network with the data traffic. Each node before forwarding a packet uses this trust information to find the most trustworthy path. Direct trust is computed based on [17]. The limitations and future enhancements of the proposed solution are same as mentioned for paper [17].

K. TR-DSR: A routing Protocol Based on Trust

C. Wang *et al.* [19] proposed a routing algorithm tr-DSR, which is extended DSR. The algorithm returns the routes having higher trust rather than shortest path. The process flow of the protocol is shown in fig. 5. In the proposed algorithm some of route replies are redundant and the number of route request re-broadcasts can be reduced by allowing only legitimate nodes to rebroadcast the route requests.

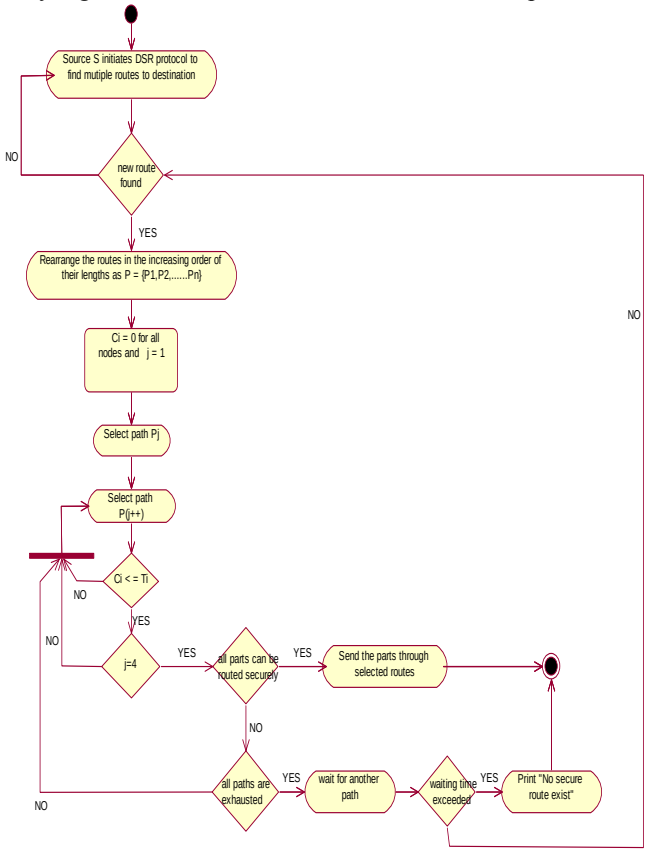

Fig. 8. Process Flow for soft encryption & trust based routing protocol.

L. Multi-path and Message Trust-based Secure Routing

S. K. Dhurandher and V. Mehra [23] proposed a trust based routing which protects the message against modification. In this, trust is calculated in a dynamic way and less trusted path may also be used to transmit data depending upon the security requirement of the message. It makes use of an encryption technique not requiring intensive computations. Before selecting the final paths, source waits for RREP from different paths and if all the paths have trust less than the required trust, the message is divided, encrypted and then sent. This increases the delay in routing.

M. FACES: Friend-Based Routing Protocol

In FACES [24], trust of the nodes is determined by sending challenges and sharing friends' lists. The proposed algorithm is divided into four stages: Challenge your neighbor, Rate friends, Share friends and Route through friends. Challenges are sent to authenticate the nodes. Nodes which complete the challenge are put into the friend list and otherwise they are put into the question mark list. In rate friends stage friends rating is done on the basis of the amount of data they transmit and rating obtained by other friends. This protocol requires that each node stores different lists.

N. Trust-Based on-Demand Multipath Routing Protocol

X. Li *et al.* [25] proposed AOTDV routing protocol. Here, trust of a node is represented as a weighted sum of forwarding ratio and path trust is computed as a continued product of node trusts. Here, the node is considered as malicious based on its forwarding behavior. Misbehaving nodes may participate in the Route Discovery but may refuse to forward the data packets. So, for calculating Trust of such a node, Control packet Forwarding Ratio, CFR (t) value can be given less weight than Data packet Forwarding Ratio, DFR (t) value.

IV. Comparison

TABLE I: The Highlighting Features, Requirements and Limitations of The Trust Based Secure Routing Protocols

Protocol	Highlighting Features	Requirements	Weaknesses/ Overheads
T. Ghosh *et al.* [12]	isolates malicious nodes acting independently or in collusion	requires the existence of a Public Key Infrastructure	increases delay in Route Discovery
T. Ghosh *et al.* [13]	model also works for colluding malicious nodes	all the nodes have identical radio range, requires Public Key Infrastructure	malicious node sends false accusation message, increases delay in Route Discovery
Pirzada *et al.* [14]	Works without requiring trust infrastructure		Nodes work in promiscuous listening mode
Pirzada *et al.* [15]	Intermediary nodes act as Trust Gateways	Trust Gateway nodes should not be malicious	Nodes work in promiscuous listening mode
Pirzada *et al.* [16]	The trust model makes use of trust agents that reside and run on each node	nodes do not collude, uses promiscuous mode for trust assignment	increases the delay in route discovery as well as the resulting returned route may be long
Pirzada *et al.* [17]	divided into three components: Trust agent, Reputation agent and the Combiner	Assumes that nodes do not have varying transmission power	uses promiscuous mode for trust assignment, trust is based solely on the forwarding behavior
Pirzada *et al* [18]	Each node monitors it's neighbors and update trust	Assumes that nodes do not collude	Nodes work in promiscuous mode, trust is based on the forwarding behavior
C. Wang *et al.*	reduces routing traffic by forwarding	Solution uses pre computed trust values	some of route replies are redundant

[19]	requests to selected nodes		
TAODV [20]	trust is represented by opinion as used in subjective logic	requires the nodes to authenticate each other by verifying the certificate	unable to detect in case a malicious node authenticates itself but later on acts as a blackhole
DMTR [21]	contains three components: the Requestor, the Decision Maker and the Executant	Uses Trust Network Connect (TNC) and barrel theory	Exchange of trust table between nodes requires lots of bandwidth
P. Narula *et al.* [22]	It uses soft encryption techniques	No. of encrypted parts given to a node depends upon trust value	takes more time in route selection
Dhurandher *et al.* [23]	trust is calculated in a dynamic way	Uses less intensive encryption	increases the delay in routing
FACES [24]	can handle many attacks	Incorporates Friend-based mechanism	
AOTDV [25]	meets the trust requirement of the data packets	neighbors are evaluated using packet forwarding ratio	Misbehaving node may not give true Path Trust in case of colluding attack

V. Conclusion and Future Scope

This paper discusses the different trust based secure routing protocols. The protocols [16]-[18] fail to work when malicious nodes collude. Protocols proposed in [12], [13], [15]-[18], [20], [25] require each network node to work in promiscuous mode, increasing the network overhead and requires nodes to have high energy capacity as they need to overhear all the transmissions. The protocols in [12], [16], [23] increase delay in route discovery and the solution in [16], [19] result in the most trustworthy path but do not discover the shortest path. Protocol [18] requires each node to have high memory capacity as they store large tables. There may be other reasons that a node does not behave normally like low energy, congestion in the network, lossy links, destination has moved etc. The existing protocols do not check for these reasons before declaring a node's behavior as malicious. So there is a need to design a secure trust based routing protocol which overcomes limitations of the existing routing protocols without compromising the network performance and the solution must consider resource constraints in terms of computation, energy, communication, and memory.

References

[1] L. Zhou and Z. Haas, "Securing ad hoc networks," *IEEE Netw.*., vol. 13, Issue 6, pp. 24-30, 1999.

[2] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proc. 3rd ACM workshop WiSE*, pp. 1-10, Sep. 2002.

[3] P. Papadimitratos and Z. Haas, "Secure data transmission in mobile ad hoc networks," in *Proc. ACM workshop WiSE*, pp. 41-50, Sep. 2003.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. Sixth Ann. Int'l Conf. Mobile Computing and Networking (MobiCom)*, pp. 255-265, 2000.

[5] S. Buchegger and J. Boudec, "Performance analysis of the confidant protocol: cooperation of nodes—fairness in distributed ad hoc networks," in *Proc. IEEE/ACM Workshop Mobile Ad Hoc Networking and Computing (MobiHOC)*, pp. 226-236, 2002.

[6] K. Sanzgiri, B. Dahill, B. N. Levine, E. M. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," in *Proc. International Conference on Network Protocols (ICNP),* IEEE Press, pp. 78–87, 2002.

[7] Y.C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," in *Proc. 4th IEEE Workshop Mobile Comp. Sys. And Applications*, pp. 3-13, Callicoon, NY, June 2002.

[8] Y.C. Hu, A. Perrig and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *Proc. Eighth Annual International Conference on Mobile Computing and Networking (MobiCom)*, ACM Press, pp. 12-23, 2002.

[9] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad-hoc wireless networks," in *Mobile Computing*, T. Imielinski and H. Korth, Eds., Kluwer, pp. 153-181, 1996.

[10] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *Comp. Commun. Rev*., pp. 234-44, Oct. 1994.

[11] A. Perrig, R. Canetti, D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA CryptoBytes* vol. 5, no. 2, 2002.

[12] T. Ghosh, N. Pissinou, and K. Makki, "Collaborative Trust-based Secure Routing Against Colluding Malicious Nodes in Multi-hop Ad Hoc Networks," in *Proc. 29th Annual IEEE International Conference on Local Computer Networks*, pp. 224-231, 2004.

[13] T. Ghosh, N. Pissinou, and K. Makki, "Towards Designing a Trusted Routing Solution in Mobile Ad Hoc Networks," *Mobile Networks and Applications, Springer Science*, vol. 10, pp. 985-995, 2005.

[14] A. A. Pirzada, A. Datta, C. McDonald, "Trust-based routing for ad-hoc wireless networks," IEEE, pp. 326-30, 2004.

[15] A. A. Pirzada and C. McDonald, "Deploying trust gateways to reinforce dynamic source routing," in *Proc. 3rd International IEEE Conference on Industrial Informatics*, IEEE Press, pp. 779-784, 2005.

[16] A. A. Pirzada and C. McDonald, "Trust Establishment In Pure Ad-hoc Networks," *Wireless Personal Communications*, Springer, pp. 139–163, 2006.

[17] A. A. Pirzada, Amitava Datta, Chris McDonald, "Incorporating trust and reputation in the DSR protocol for dependable routing," *Computer Communications*, vol. 29, issue 15, pp. 2806-282, 5 September 2006.

[18] A. A. Pirzada and C. McDonald, "Dependable dynamic source Routing without a trusted third party," *Journal of Research and Practice in Information Technology*, vol. 39, issue 1, February 2007.

[19] C. Wang, X. Yang, and Y. Gao, "A Routing Protocol Based on Trust for MANETs," *Springer-Verla*, 2005, pp. 959–964.

[20] X. Li, M. R. Lyu, and J. Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks," in *Proc. Aerospace Conference*, IEEE, vol. 2, pp. 1286-1295, 2004.

[21] C. Huang, Y. Cheng, W. Shi, H. Zhou, "A Trusted Routing Protocol for Wireless Mobile Ad hoc Networks," in *Proc. IET Conference on Wireless, Mobile and Sensor Networks (CCWMSN07)*, pp. 406-409, Dec. 2007.

[22] P. Narula, S. K. Dhurandher, S. Misra, and I. Woungang, "Security in mobile ad-hoc networks using soft encryption and trust based multipath routing," *Sci. Direct Comput. Commun*., vol. 31, pp. 760-769, 2008.

[23] S. K. Dhurandher and V. Mehra, "Multi-path and message trust-based secure routing in ad hoc networks," in *Proc. Int. Conf. Advances in Computing, Control and Telecomm.Technologies*, pp. 189-194, 2009.

[24] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta, and P. Dhurandher, "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems," *Systems Journal*, IEEE, Vol. 5, Issue 2, pp. 176-188, 2011.

[25] 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.

Deepika Kukreja is a PhD candidate in the field of Mobile Ad Hoc Networks at University School of Information and Communication Technology, GGSIP University, Delhi, India. Deepika received her Master of Technology in Computer Science and Engineering from YMCA, Faridabad, Haryana, India. She is working as an assistant professor at Maharaja Agrasen Institute of Technology, GGSIP University, Delhi, India. Her research interests include Computer Networks, Routing in Wireless Networks and Security in Ad Hoc Networks.