Inclusive Survey of Various Trust based Dynamic Source Routing Protocol for Mobile Ad-hoc Network

Priya Kautoo
Deptt. of CSE, UIT, RGPV
Bhopal, MP, India

Piyush Kumar Shukla
Deptt. of CSE, UIT, RGPV
Bhopal,MP, India

Sanjay Silakari
Deptt. of CSE, UIT, RGPV
Bhopal, MP, India

ABSTRACT

An ad-hoc network is a set of mobile nodes in which it is required that each node performs cooperatively and a node is called cooperative when it transfers data correctly to another node in a wireless network. But due to openness in ad-hoc network, it is vulnerable to various kinds of attack from malicious nodes. Various routing protocol recently have been projected to perform secure routing. For the identification of malicious nodes in mobile ad-hoc network trust based reactive routing protocol are typically used and consequently achieved results are far better. This paper surveys totally different trusted Dynamic source routing protocol, and it is analyzed that the dynamic source routing protocol performs better, whenever the thought of trust being placed in the straightforward dynamic source routing protocol.

Keywords

DSR, Malicious, Prediction, Reliability, Trust.

1. INTRODUCTION

Mobile ad-Hoc network [1] is a collection of mobile devices or nodes that can communicate without any infrastructure (like access point or base station) or predefine network topology. Dynamic network topology, Multi-hop routing, Device heterogeneity, Limited Bandwidth, Limited physical security Self-creation, self-organization and self-administration, openness and low transmission range are the main characteristic of mobile Ad-Hoc network. Due to these characteristic mobile Ad-Hoc network is vulnerable to various kinds of attack from malicious node [2, 3].

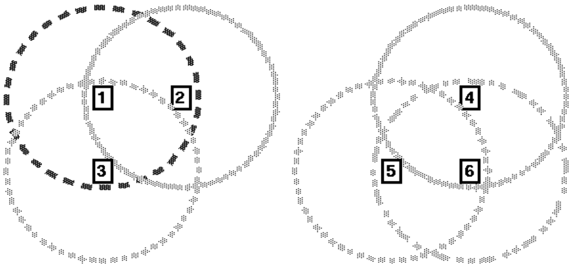

Fig. 1: Simple Example of Mobile Ad-Hoc Network

1.1 Routing in MANET

Routing in mobile Ad-hoc network is basically different from traditional routing to originate on the infrastructure network [5]. Routing in the mobile Ad-hoc network depends on many criteria, which involve topology selection, route selection, initiation of request and specific underlying characteristic. Several routing protocols have been invented for mobile Ad-Hoc network.

These routing protocols can be classified into two types.

(a) Proactive Routing Protocol

(b) Reactive Routing Protocol

Proactive routing are also known as table driven routing protocol in which all nodes in a MANET should keep track of route to all potential targets so that when a packet needs to be forwarded, the route was previously known and can be directly used. In proactive routing each node exchange route information periodically or in the response to topology changes. There are several proactive routing protocols such as DSDV, CGSR [6]. The main drawback of the proactive routing protocol is to maintain the routing table periodically, and it increases routing overhead. On the other hand, the reactive routing protocol encompasses a lazy method to discover the route, in its node only discovers routes when it is needed that's why this routing protocol is also known as on demand routing protocol. AODV, DSR are the example of reactive routing protocol.

These all routing protocols suffer from attack by malicious nodes. To secure routing protocol several secure routing protocols are launched such as SAODV and Ariadne. But these both routing protocol requires a trusted third party or centralized unit. The common trusted authority violates the nature of self-organization. This routing protocol is not practical for MANET. Therefore, security is the key concern for MANET. Security for the MANET comes from both failure of mobile devices and subversion to these devices by enemies. Mobility also makes physical security more difficult as the negotiation of a valid node or the addition of a malicious node may go unobserved in such a dynamic environment.

A new class of routing protocol is in trend now a day; these protocols are based on trust and these are known as trust based routing protocol [7, 8, 9, and 10]. Trust is a complex subject related to the belief in honesty, truthfulness, completeness, reliability, etc. of an entity. According to Kimi and choohineh trust is "belief that is influenced by the individual opinion."

1.2 Types of Attacks in MANET

(a) Internal Attack
(b) External Attack
In internal attack, the attacker wants to gain access to the network and also wants to participate in the network activities. Internal attackers are the node that has been compromised by malicious parties. An internal attacker announces fake routing information in order to misroute the flow of information in the network. Generating gray hole, black hole [4], warm hole, flooding or denials of service attacks are the most commonly

used internal attack in MANET. On the other hand, External attacker tries to interrupt the network by injecting erroneous routing information so in the external attack the main aim of the attacker is to cause overhead in the network. To resolve the problem of external attacks various encryption techniques are often used, but this solution still looked-for further supervision mechanism such as centralized trusted third party to implement secret key distribution, authorization and data signature. But this solution to resolve the external attack is inappropriate for pure mobile Ad-Hoc network because it requires a trusted third party and this solution shows inefficiency in handling the attack from internal malicious nodes which may influence on the security the confidentiality and life cycle of the entire network.

Table I. Attacks Corresponding to Different Layer in MANET

Layer of MANET	Type of attack
1.Attack at application layer	1. Negation attack
	2. Attack by Virus and Worms
2.Attack at transport layer	1.TCP SYN attack(Denial Of Service attack)
	2.TCP Session Hijacking
	3.Jelly Fish attack
3. Attack at network layer	1.Flooding Attack(Denial Of Service attack)
	2.Route tracking
	3.Message Fabrication, Alteration
	4.Black hole attack
	5.Worm hole attack
	6.Line Spoofing attack
4. Attack at MAC layer	1.Traffic Alteration and analysis
	2.MAC denial of service attack
	3.Bandwidth Stealth
	4.MAC targeted attack
	5.WEP targeted attack
5.Attack at physical layer	1.Jamming attack
	2.Compromised attack
	3.Malicious message injection
	4.Eavesdropping attack

Trust prediction mechanism allows a node to evaluate trustworthiness of other node which not only help in the detection of malicious node but also improve network performance and robustness. In this paper we classified the trust into two types-Direct Trust and Recommending Trust. Direct trust is the first hand information of the neighborhood node on the other side recommending trust is the second handinformation of neighbor. The main objectives of this paper are (a) To increase network security, (b) To protect the network from internal attack,(c) Improve the trust factor and to compare several DSR routing protocol. The remaining paper is organized in the following manner. Literature review is discussed in section 2. Section 3, describes trust based dynamic source routing protocol in detail. Finally,Section 4 gives the concluding comments in addition to extensions and directions for future research.

2. LITERATURE REVIEW

Several researches have been done to enhance the security, misbehavior detection as well as trust management in mobile Ad-hoc network. This Literature survey encompasses several trust models and trust based routing for Dynamic Source Routing protocol. DSR uses source routing that is why several new routing protocols have been developed for DSR [11, 12]. At the end of the survey a comparative study of these protocols is performed in Table 1.

2.1 Watchdog and Pathrater

The thinking on concept of Trust in DSR is started from 2000 with adding watchdog and pathrater mechanism in simple DSR protocol by Mortiet. al. [13,14] Watchdog is responsible for detection of malicious node and path rater avoids routing through these nodes. In this scenario, some nodes are considered as preauthorized, called as anchor node. The main drawback of this protocol is that routing through the malicious node is avoided and it does not do anything to penalize them.

2.2 CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc Network)

Further then CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc Network) protocol have been proposed by Buchegger et al. [15,16] this protocol adds the concept of trust management, reputation system and punishment mechanism in Watchdog and Pathrater mechanism. When a node uses this routing mechanism, each node maintains four components- a monitor, a reputation system, trust manager and a path manager. The monitor is responsible for detection of misbehaving or malicious node. On the bases of observed behavior, reputation system calculate the reputation of each node. Trust manager exchanges trust alert with the other neighbor trust managers. Ranking of the path and the validity of path is maintained by path manager. This protocol is vulnerable from black hole attack because in punishment mechanism, data packet never forwarded through black listed node.

2.3 A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks

After that CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks, CONFIDANT protocol allows a node to exchange both positive and negative reputation to their neighbor overcome this problem CORE protocol has been proposed. The working of CORE routing is similar to CONFIDANT routing protocol, only difference is that CORE allows only to exchange the positive observation among the nodes and it does not suffer from a black hole attack.

2.4 Trusted DSR

CHENG Yong et al. [17] extend DSR to trusted DSR and employs the idea of Trust Network Connect (TCN). For trusted DSR Trust score is used for representation of trust of each node, which includes direct trust and indirect trust. Trust association and route selection are based on experience observed or stated routing and forwarding activities of other node.

2.5 Secure-AODV and Ariadne

Y-C Hu et al. propose secure-AODV and Ariadne [13], which are secure on-demand routing protocol. Both of these routing protocol needs a centralized authority for maintaining trust relationship between nodes. Due to the necessity of centralized authority these protocols are not appropriate for MANET.

2.6 Incorporating Trust and Reputation in the DSR Protocol for Dependable Routing

Pirzada et al. [18] proposed a trust based DSR routing protocol in which trust among the nodes is maintained according to reputation of each node. This protocol combines the working of simple DSR with a Trust model. The Trust model contains three components – Agent, Reputation Agent and the Combiner. Trust agent is responsible for the determination of Trust level or reputation of each node on the basis of directly experienced activity of nodes. The reputation agent exchanges the trust information among the nodes in DSR route discovery phase. Thus trust agent and reputation agent sends the direct trust value and reputation value respectively to the combiner. Finally, combiner evaluates the cumulative sum of trust value.

2.7 Trust Management Model for Mobile Ad-hoc Network Based On Analytic Hierarchy Process and Fuzzy Theory

Fuzzy based trusted dynamic source routing protocol have been proposed by H. Xia et al [19]. This trust model uses the concept of analytic historical theory (AHT) for the computation of trustworthiness of each node and the node future trust is evaluated by Fuzzy theory. The main drawback of this routing protocol is that it requires to exchange recommendation among nodes i.e. routing overhead is very high for FTDSR.

2.8 Trust Prediction and Trust-based Source Routing in Mobile Ad-hoc Networks

Xia et al [20] has proposed a routing protocol named as trusted source routing protocol (TSR). In TSR, trust among nodes is classified into three categories – Node historical trust, node current trust and the route trust.Node historical trust is computed with the help of packet forwarding ratio and the node future trust is predicted with the help of fuzzy prediction theory. TSR improves the throughput and packet forwarding ratio when compared with other DSR routing protocols.

From the survey it is analyzed that the performance of Dynamic Source Routing Protocol increases when it uses the security mechanism and it is also analyzed that the performance of DSR is higher when the concept of trust is fortified with it.

3. KEY PERFORMANCE INDICATORS

(1) **Packet Forwarding Ratio-** It is the ratio between total numbers of packet forwarded correctly to the total number of packet forwarded.

$$\text{Packet forwarding ratio} = \frac{\text{No. of packet forwarded correctly}}{\text{Total no. of packet forwarded}}$$

(2) **Packet Drop Ratio:** It is the ratio between total numbers of packet dropped to the total number of packet forwarded.

$$\text{Packet Drop Ratio} = \frac{\text{No. of packet dropped}}{\text{Total number of incoming packet}}$$

(3) **Network Throughput:** Throughput indicates the total amount of information transmitted per second from source to destination.

(4) **Packet Delivery Ratio:** It is the proportion of total number of data packet delivered to the destination node to the total number of data packets sent by the source node.

$$\text{Packet Delivery Ratio} = \frac{\text{Total number of data packet delivered to the destination}}{\text{Total number of data packets sent by the source node}}$$

(5) **Routing Packet Overhead:** It is the ratio between control packets (including route request, route reply, and route update and error packet) to the data packet.

(6) **Packet Modification Ratio:** It is the proportion of total number of packet modified to the total number of incoming packet.

$$\text{Packet Modification Ratio} = \frac{\text{Number of packet modified}}{\text{Total number of incoming packets}}$$

(7) **Packet Misroute Rate:** ratio between numbers of packet misroute to the total no of packet forwarded to the destination.

$$\text{Packet Misroute Ratio} = \frac{\text{Number of packet misroute}}{\text{Total number of packet forwarded}}$$

(8) **Average end-to-end latency:** Average end to end latency can be define as the average time taken by the source node to transfer the data packet to the destination node. And end to end latency include all types of delay such as buffer delay, delay during route request message, delay during retransmission of the data packet, and propagation time etc.

(9) **Path Optimality:** It is the ratio between total numbers of Hopes in the shortest path to the one of the Hope in the path taken by data packet.

Table II. Comparative Study of various DSR Routing Protocol

Name of Protocol	Features							
	Routing Mechanism	**Route Configuration Mechanism**	**Multi-cast Capability**	**Type of Trust Used**	**Packet Loss Ratio**	**Throughput**	**Routing Overhead**	**Packet Forwarding Ratio**
DSR	Shortest path	Erase Route, notify source	No	Not use	Highest	Low	Low	Low
Watchdog and pathrater	Shortest path	Source avoid routing through the malicious node	No		Lower then DSR	Higher then DSR	High	Better then DSR
CONFIDANT	Shortest path	Implement a punishment based mechanism	No	Add trust manager & reputation system	Lower then Watchdog & pathrater	Higher then Watchdog& pathrater	High	Good
CORE	Shortest path		No		Lower then CONFIDANT	Higher then CONFIDANT	High	High
Trusted DSR	Shortest path+max trust value	Best effort delivery	No	Direct	30% improved as DSR	Higher then DSR	Low	High
Trust Based DSR	Shortest path+Direct Trust Value	Avoid routing through malicious node	No	Direct	Low	Higher then DSR	Low	Good
SADSR	Shortest path+max trust value	Authenticate message using asymmetric cryptography	No	Not Use	Higher then TDSR	Lower then TDSR	High	High
Ariadne	Shortest path which contain authenticated route	Authenticate message with symmetric cryptography	No	Not use	Lower then TDSR	Higher then TDSR	High	High
FTDSR	Shortest path on the bases of max forwarding ratio	Sends route error message to the source	No	Both direct & indirect	Lower then TDSR	Higher then TDSR	Low	High
TSR	Shortest path	Same as FTDSR	No	Both direct & indirect	Lowest	Higher then FTDSR	Lowest	Highest

4 . TRUST BASED DSR PROTOCOL

There are two types of Trust value is used for Trust based Dynamic Source routing protocol.

- **Node Historical Trust:** Node Historical Trust is computed by observing neighborhood behavior based on historical interaction information. In this model Packet Forwarding ratio

[15, 16] is the single scalar factor which is use for calculation of trust. For the evaluation of trust value of monitored node basically two Trusts factor are used which are Control Forwarding Ratio and Data Forwarding Ratio.

- **Route Trust:** Route trust value is computed on the basis of the intermediate node's trust value along the path between source nodes to the destination node. All of the decisions such as whether packet is forwarded or not is depend on the Route Trust value.

4.1 Protocols Detail

A novel trusted Dynamic Source Routing protocol is described in this portion and is extended from source routing Mechanism. In Trusted DSR routing [20, 21] is done in two phases

(a) Route Discovery/ Path Selection
(b) Route Maintenance/Update

Route discovery [22] is done when source node wishes to transfer packet or data to the destination node. The entire process of route discovery and path selection in done as follows:

- When source node have a data packet for destination before sending the packet source node checks its local routing cache table whether it has route from source node to the intended destination node and when appropriate path exist in the local cache it compare the trust value of qualified route to the required route trust value of data packet. If qualified route trust value is greater than required route trust limit then source node sends the packet.

- When no such path exists in the route cache of the source node, the source initiates route discovery and path selection process. When more than one path is found for a single route discovery, then all of these route entries are entered into the route cache table of the source node.

- If a number of routes fulfill the required trust limit then the source node selects the routes which have the smallest hop-count.

- The route with the maximum route trust will be selected when more then one routes have equal hop count and meet the trust requirement.

5. CONCLUSION

During this paper, a survey of various Trusted Dynamic source routing protocol have been done, and it is analyzed that the performance of dynamic source routing protocol will increase, whenever the thought of trust being place to the straightforward dynamic source routing protocol and this paper conjointly tries to look attotally different attacks, that occurred in various layers of mobile Ad-Hoc network. DSR protocol is selected because it uses the concept of routing cache for route discovery. However, still it needs a lot of work to increase the trustworthiness of reactive routing protocol.

6. REFERENCES

[1] D. V. Viswacheda, M. S. Arifianto and L. Barukang, "Architectural Infrastructural Issues of Mobile Ad hocNetwork Communications For Mobile Telemedicine System, "4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications March, 2007, pp. 22-29.

[2] Anuj Joshi1, PallaviSrivastava and Poonam Singh "Security Threats in Mobile Ad Hoc Network" 2010 S-JPSET,:, Vol. 1, Issue 2, ISSN: 2229-7111.

[3] Mohammad Wazid, Rajesh Kumar Singh, R. H. Goudar "A Survey of AttacksHappenedatDifferentLayers of Mobile Ad-Hoc Network &SomeAvailableDetection Techniques" Proceedingspublished by International Journal of Computer Applications® (IJCA) International Conference on Computer Communication and Networks CSI- COMNET-2011.

[4] Mrs. KritikaTaneja, Dr.S.S.TYAGI, "security issue on aodvroutingprotocolsufferingfromblackholeattack"International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) Volume 1, Issue 7, September 2012.

[5] Azzedine Boukerche, BegumhanTurgut, NevinAydin, Mohammad Z. Ahmad, LadislauBölöniDamlaTurgut "Routingprotocols in ad-hoc networks: A survey," Elsevier Computer Networks 55 (2011) 3032–3080.

[6] Nikola MilanovicMiroslawMalek, Anthony Davidson, VeljkoMilutinovic "Routing and Security in Mobile Ad Hoc Networks" Published by the IEEE Computer Society 2004.

[7] Asad Amir Pirzada, AmitavaDatta, Member, Chris McDonald "TrustworthyRoutingwith the AODV Protocol"Published by the IEEE Computer Society 2004.

[8] X. Li Z. Jia P. Zhang R. Zhang H. Wang "Trust-based on-demandmultipathrouting in mobile ad hoc networks" Published by The Institution of Engineering and Technology 2010.

[9] Hui Xia, ZhipingJia, Lei Ju, XinLi, Edwin H.-M. Sha"Impact of trust models on-demand multi-pathrouting in mobile ad-hoc networks"Computer Communications 36 (2013) 1078–1093.

[10] K. Garg, M. Misra "Trust Based Multi Path DSR Protocol," International Conference on Availability, Reliability and Security 2010.

[11] D. Johnson, D. Maltz, "Dynamic source routing in ad hoc wireless networks," in: I. Tomasz, K. Hank (Ends.), Mobile Computing, first ed., Kluwer AcademicPress, 1996, pp. 153–181.

[12] Surya Kant, Dr. KrishanKumar "Performance Analysis Of Dynamic Source Routing Protocol In Wireless Mobile Ad Hoc Network" International Journal of Engineering Research&Technology (IJERT) Vol. 1 Issue 10, December- 2012 ISSN: 2278-0181.

[13] Asad Amir Pirzada, AmitavaDatta, "A Trust Model BasedRouting Protocol for Secure Ad Hoc Networks" Member IEEE, Chris McDonald 2004.

[14] S. Marti, T.J. Giuli, K. Lai, M. Baker, "Mitigatingroutingmisbehavior in mobile ad-hoc networks," Mobile Computing and Networking (2000) 255–265.

[15] S. Buchegger and J.-Y. Le Boudec, “Performance analysis of theconfidantprotocol,” in MobiHoc ’02: Proceedings of the 3rd ACMinternational symposium on Mobile ad hoc networking &computing. New York, York, NY, USA: ACM, 2002, pp. 226–236.

[16] Sonja Buchegger and JeanYves Le Boudec “Performance Analysis of the CONFIDANT Protocol(Cooperation Of Nodes: Fairness In Dynamic Ad-hocNetworks)” EPFL Lausanne, Switzerland. June 2002.

[17] CHENG Yong, HUANG Chuanhe, SHI Wenming “TrustedDynamic Source Routing Protocol” Published by the IEEE Computer Society 2007, 1623-1636.

[18] Asad Amir Pirzada *, AmitavaDatta, Chris McDonald “Incorporating trust and reputation in the DSR protocol for dependablerouting” Computer Communications 29 (2006) 2806–2821

[19] H.Xia,Z.Jia,L.Ju,Y.Zhu, “Trust management model for mobile ad-hoc network based on analytichierarchyprocess and fuzzytheory”Published in IET Wireless Sensor systems2011.

[20] Hui Xia, Zhipingjia, Xin Li, Lei ju “Trust Prediction and Trust-based source routing in mobile ad hoc networks” Computer Communications 2012

[21] .RaihanaFerdous, VallipuramMuthukkumarasamy, Abdul Sattar “Trust Formalization in Mobile Ad-Hoc Networks” 2010 IEEE 24th International Conferenceon Advanced Information Networking and Applications Workshops 351-356.

[22] Asad Amir Pirzada, Chris McDonald “Trusted Route Discoverywith TORA Protocol” Published by IEEE 2004.

.

AUTHORS PROFILE

Priya Kautoo: received her Bachelor`s degree in Computer Science and Engineering, GGCT, Jabalpur, India in 2010.At present she is pursuing her M.E. degree in Computer Science & Engineering from UIT-RGPV, Bhopal India. Her research areas are Computer Networks, Security in Ad-Hoc Network.

Dr. Piyush Kumar Shukla: received his Bachelor’s degree in Electronics & Communication Engineering, LNCT, Bhopal in 2001, M. Tech (Computer Science & Engineering) in 2005 from SATI, Vidisha and Ph.D. (Computer Science & Engineering) in 2013 from RGPV, Bhopal. M.P. India. He is a member of IACSIT, IAENG. Currently he is working as an Assistant Prof. in Department of Computer Science & Engineering, UIT-RGPV Bhopal. He is also I/C of PG Courses in DoCSE, UIT, RGPV. He has published more than 40 Research Papers in various International & National Journals & Conferences.

Dr. Sanjay Silakari: received his Bachelor’s degree in Computer Science & Engineering from SATI, Vidisha in 1991, M.E. (Computer Science & Engineering) from DAVV, Indore in 1998) and Ph.D. (Computer Science & Engineering) in 2006 from B.U. Bhopal (M.P.) India. He has published more than hundreds Research Papers in various International & National Journals & Conferences. He is Dean of Faculty of CSE & IT in RGPV. Currently He is working as Joint Director in UIT-RGPV and Prof. & Head in CSE Department, UIT-RGPV Bhopal. He is also member of various Academic Societies. He is Life Member of ISTE