International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 9, ISSN No. 2455-2143, Pages 102-107
Published Online January 2018 in IJEAST (http://www.ijeast.com)

REVIEW OF ROUTING PROTOCOL BASED ON TRUST IN MANET

Vijay Kumar Singh
Dept. of CSE
JNCT,
Bhopal, Madhya Pradesh, India,

Dr. Piyush Kumar Shukla
Dept. of CSE,
University Institute of Technology, Bhopal,
Madhya Pradesh, India

Dr. Sachin Goyal
Department of Information Technology,
University Institute of Technology, Bhopal, Madhya Pradesh, India

Abstract - The ad-hoc network is required when two or more wireless mobile nodes wish to transfer packet/data to other nodes. Dynamic source routing protocol (DSR) is widely used in an ad-hoc network routing through DSR is also suffered from attacks through malicious nodes. This is very difficult to identify these venomous nodes, adding trust is good in the routing process helps. Some papers on the same topic have been discussed here.

Keywords- Ad-Hoc Network, Attack, DSR, Malicious, SVM

I. INTRODUCTION

The landscape of the network security [1] has changed with the rapid development of wireless network [2] and mobile computing applications [3]. Most of the proven security mechanism becomes inefficient because of the new features of mobile ad-hoc network [4], i.e. mobility and infrastructure less architecture [5]. These features increase the vulnerabilities and routing challenges [6] that do not exist in fixed wired networks. Now a day's network security [7] is an interesting research area for many researchers for secure and fast communication [8] over the Internet. In last few year communications over MANET [9] is secure by some key management schemes, but it requires some authentication and encryption [10] mechanism that mean these solutions needed some authenticated trusted third party for issuing digital certificates, which disturbs the nature of the MANET [11].

II. MOTIVATION

In MANET when a node wishes to transmit a packet (data/control) to another node, but the intended node does not belong in its one hop neighbor [20], then it has to rely to the intermediate node to forward the packet. This mechanism is known as multi hop. Current investigation designates that the wireless ad-hoc network [21] is more vulnerable than the conventional wired and wireless networks due to its underlying features of open medium, dynamic network topology [22], limited bandwidth, distributed cooperation and restricted energy resources. Thus, well-organized routing protocols are required in order to enhance the communication and several routing protocols to have been proposed for MANET [23]. They are mainly classified under two categories proactive and reactive routing protocol, former is the table driven routing protocol [24] in it all the routes to destinations or for other node is pre-determined and preserved in the episodic update process. In proactive, routing protocol routes are created on the fly or when needed [25]. These all traditional protocols to attack by malicious nodes because they do not encompass any security mechanism. Recently, a new class of routing protocol has been proposed known as trust based routing protocol [26] for secured routing.

III. RELATED WORK

Trust Models in MANE: Due to mobility and openness mobile ad-hoc network is vulnerable to several types of attacks from malicious nodes. To secure MANET from such as the malign nodes, a new kind of security mechanism has been proposed, which uses the concept of trust. Several trust models have been proposed, which are used before the conjunction with routing protocol.

Distributed Trust Model [1997]: The distributed trust model uses a decentralized approach for trust management [8]. For this, model trust is represented in the form of trust level, and these trust levels are computed through different trust categories and trust value. The trust level ranges from -1 to 4 where -1 define complete distrust, and 4 define accomplished trust. This model also allows a protocol to exchange, revoke and refresh recommendation [27] about entities. For a unique target, this model has the provision of multiple recommendations and uses the cumulative sum to determine a single [28] recommendation.

Drawback: This model is not more suitable for ad-hoc network [1, 3] because it requires that recommendation about another entity to be passed and management of false or malevolent recommendation.

Drawback: This model cannot work properly with MANET because it requires an extensive pre-configuration of the servers and distributed central authority [9, 11].

*Role and Reputation Based Trust Management [2002].*N N Li et al. [10] proposes a role-based trust management framework (RBTM) for mobile ad-hoc networking. RBTM is the combination of role-based access control and trust management system and is especially suitable for attribute based access control. This trust model is working with two assumptions: in the network, there is RBTM allow them to access according to their role. Role and reputation system is also discussed in paper [11].

*Hybrid Trust Management System [2011].*The The Hybrid Trust Management System has been proposed by Rehan Akbaniet. Al. [12] is a combination trust management of the role based and reputation based trust model. A centralized authority assigns roles to each entity in HTMS, and then each role is assigned with minimum and maximum privilege levels. The privilege level of a node is determined by the score of role and reputation.

Advantage: This model allows spontaneous, fine grained access to the network resources on the basis of node's behavior.

Fuzzy Based Trust Model [2010]: Luo and fan et. al. [13] has proposed a subjective trust management model based on a certainty-factor for mobile ad-hoc network (CF Strust). This model considers fuzzy set theory and reputation model, which can be used to make significant and evaluate the credibility of nodes. Fuzzy likelihood estimation [11, 13] is used to store the problem of trust management. This model gave and defines the trust evaluation mechanism and the derivation rule for the recommendation trust [12, 14] relationship. Although two significant factors with mathematical derivation are presented in this model, but it did not take understandable account of the node computing power [15, 17], the transmission of information inconsistency and the fluctuation problem of trust [19, 21].

An SVM-based Misbehavior Detection and Trust Management Framework for Mobile Ad-hoc Networks *[2011]*. Wenjia Li et al [14] has been proposed An SVM-based Misbehavior Detection and Trust Management Framework for Mobile Ad hoc Networks (SMART), is a multidimensional trust management scheme [20, 22]. This trust model does not use any predefine threshold value for trust computation because a smart attacker [23, 24] can easily alter the threshold. This model uses Support Vector Machine for the classification of nodes. SMART framework can be easily applied in the mobile ad-hoc network [25, 27].

3.2 ***Several secure/trusted routing protocol. Cooperation of Node Fairness in Dynamic Ad-hoc Networks*** *(CONFIDANT) [2002]***.** Sonja Bucheggeret. Al. [15] has proposed CONFIDANT (Cooperation of node fairness in dynamic ad-hoc networks) protocol; it adds trust manager and reputation system to the watchdog and pathrather mechanism [16, 17].]. CONFIDANT protocol is based on selective altruism and utilitarianism. In this routing protocol, trust is managed through four components: monitor, trust manager, reputation system and the path manager. This protocol makes its decision on the bases of node's reputation in the network. A possible problem with CONFIDANT protocol is that an adversary may deliberately spread false alerts to other nodes that a node is misbehaving while it is actually a well-behaved node.

Security-aware Adaptive Dynamic Source Routing Protocol (SADSR) *[2002]*. S. Ghazizadehet. Al. [18] proposed security-aware adaptive dynamic source routing protocol (SADSR). STDSR uses digital signature based on asymmetric cryptography to authenticate the routing protocol message. STDSR take the advantage of basic properties of DSR (is to have routes to each destination) and store a local trust value for each node in the network. On the bases of node trust value path trust is calculated in the route selection process and finally the path which has maximum trust value is selected for routing [28].

Trusted Ad-hoc on Demand Distance Vector Routing Protocol (TAODV) [2004].TAODV TAODV is a secure routing protocol which is an enhancement of the AODV routing protocol [1, 2, 3]. TAODV employs the idea of trust model, and the trust between nodes is derived from the term of opinion, which uses the idea of subjective logic. Opinions are not static and updated frequently. If a node performs normal behavior, its opinion from other node's point of view is incremented otherwise the node is kicked out of the entire network [4, 5, 6] as a malicious node.

Ariadne [2005]. Ariadne Ariadne Ariadne is proposed by YIH-CHUN HU et al. [20] is one of the secure routing protocols in which each routing message is authenticated using one of the following schemes: Digital signature [7, 8, 9], shared secret key between communicating node combined with broadcast authentication or shared classified key [10, 11, 12] between all pairs of nodes. Ariadne is effective, using only highly efficient symmetric cryptographic primitives. The major drawback of this protocol is that it requires trusting third party for authentication [13, 14, 15] which is impractical for MANET.

Trusted Dynamic Source Routing protocol (TDSR) *[2007]*. In Cheng Yonget. Al. [21] have proposed trusted dynamic source routing protocol, which is an extension of the DSR routing protocol. TDSR [16, 17, 18] employs the idea of Trust Network Connect (TCN) to protect the routing behavior and trust among the nodes is represented through a trust scores. For this protocol, trust is divided into two parts: Direct trust and indirect trust [19, 20, 21] and the trust values at a node are computed by an acknowledgement mechanism from source to destination. Every acknowledge increases the trust value of intermediate nodes while retransmission of acknowledgement [22, 23, 24] decreases the trust score. The drawback of this protocol is that it is impossible for the sender node to know which nodes discard the packet.

Trusted Dynamic Source Routing Protocol (ATDSR) *[2010]*.Islam tharwatet. Al. [22] propose agent based on-demand routing protocol for MANET, which uses the idea of self-monitoring. ATDSR uses dynamic source routing protocol [25, 26, 27] as underlying routing protocol. Each participating node in ATDSR routing is installed on a multi-agent system, which contains two types of agent: monitoring agent (MOA) and routing agent (ROA). In the routing process, MOA performs monitoring of its host node behavior and afterwards computes the trust value at each host node. This trust value is propagated through MOA to ROA, and then ROA finds out the most trustworthy node for a particular destination. The main advantage of this routing protocol is that it gives different possible routes with minimum overhead in terms of time delay and extra message.

Ad-hoc on demand Trusted Multipath Distance Vector Routing Protocol (AOTMDV) *[2010]*. X. Li et al. Al. [6] proposed ad-hoc on demand trusted multi-path distance vector routing protocol (AOTMDV) which extends security to AODV routing protocol. AOTMDV uses the trust prediction model to calculate the trustworthiness of the nodes and this trust prediction model uses node historical behavior and fuzzy logic rule prediction method.

Fuzzy Based Trusted Dynamic Source Routing Protocol (FTDSR) [2011].H. H. Xia et. Al. [23] Proposed fuzzy based trusted dynamic source routing protocol (FTDSR) in which trust is divided into two types: node historical trust and node current trust [28]. Node historical trust is evaluated through the analytic hierarchy process (AHP) at the end of each interval and then by applying fuzzy logic rules prediction method in the historical trust values the current trust of the node is evaluated. FTDSR performs well than DSR and TDSR routing protocol. Furthermore, for this protocol the trust estimation process only monitors the node's performance for route discovery, but not for the transmission of data packets.

Trust Based Source Routing Protocol (TSR) [2012]: Hui Xia et al. [24] extends the DSR by adding trust prediction rules for evaluation of trustworthiness of nodes. For trust based, source routing protocol (TSR) trust is divided into three parts node factual trust node current trust and the route trust. Node historical trust is computed through the packet forwarding ratio, node current trust is evaluated by fuzzy prediction rules, and the route trust is the cumulative sum of all, the node historical trust. TSR provides a flexible and reasonable approach to select the shortest route that meets the security requirement of data packet transmission. The major drawback of TSR protocol is that it uses a single scalar factors, i.e. packet forwarding ratio for trust computation.

TABLE 1: Comparison of different trusted reactive routing protocol

Authors and Year	**Name of protocol**	**Underplaying protocol**	**Security mechanism**	**Route selection mechanism**	**Route configuration mechanism**	**Multicasting capability**	**Type of trust used**

Sonja Buchegger et. al,2002[15]	Ariadne	DSR+TESLA	Uses symmetric cryptography	Select Shortest path with authenticate route	Uses routing similar as TESLA	No	Not use
S. Ghazizadeh et. al,2002 [18]	SADSR	DSR	Uses digital signature	Shortest path with	-	No	Not use
Xiaoqi Li et.al,2004[19]	TAODV	AODV	Uses idea of subjective logic	Shortest path with max. trust value	Avoid routing through malicious nodes	Yes	Direct
YIH-CHUN HU et. al,2005 [20]	CONFIDANT	-	Adds trust manager and a reputation system to watchdog and pathrather mechanism	Shortest path	Implement punishment based technique	No	Add trust manager and reputation
Islam tharwat et. al,2010 [22]	ATDSR	DSR	Uses idea of multi agent system	Shortest path with max. trust value	Best effort delivery	No	Direct
X. Li et. al,2010 [6]	AOTMDV	AODV	Uses fuzzy prediction rule	Short path on the bases of max. forwarding	Sends route error message to the source	Yes	Both direct and indirect
H. Xia et. al,2011 [23]	FTDSR	DSR	Uses fuzzy prediction rule	Short path on the bases of max. forwarding	Sends route error message to the source	No	Both direct and indirect
Hui Xia et. al.2012 [24]	TSR	DSR	Uses fuzzy prediction rule	Shortest path with min hop count	Sends route error message to the source	No	Both direct and indirect

these in combination is to fortify the trustworthiness of the route and reducing the false rate of the prediction of the route before distribution of the packet in MANET using DSR protocol.

IV. CONCLUSION

Mobile ad-hoc network is a decentralized and infrastructure fewer networks in which each node can communicate with others within the transmission range. Because of openness, mobile ad-hoc network suffered from hazard that occurred due to malicious node. To secure MANET from such hazard a new class of routing protocol has been proposed that uses the concept of trust. Previously, researchers used many techniques for the computation of trust, i.e. agent base technique, soft computing and the fuzzy prediction logical rule based methods.

V. REFERENCES

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

[2] Dilpreet Kaur and Naresh Kumar,“Comparative Analysis of AODV, OLSR, TORA, DSR and DSDV Routing Protocols in Mobile Ad-Hoc Networks” Published Online March 2013 in MECS, pp.39-46.

[3] ELIZABETHM and ROYER, CHAI-KEONG TOH, “A Review of Current Routing Protocols for Ad-hoc Mobile Wireless Networks” published in IEEE Personal Communications 1999, pp.46-55.

[4]Mehran Abolhasan a, Tadeusz Wysocki a, Eryk Dutkiewicz b, “A review of routing protocols for mobile ad hoc networks” published in Elsevier, Ad Hoc Networks 2 (2004), pp. 1-22.

[5]Sergio Pastrana, Aikaterini Mitrokotsa, Agustin Orfila, Pedro Peris-Lopez of classification algorithms for intrusion detection in MANETs”, published in science direct 2012, pp.217-225.

[6]X. Li Z. Jia P. Zhang R. Zhang H. Wang “Trust-based on-demand multipath routing in mobile ad-hoc networks," Published in IET Information Security 2010, pp.212-232

[7]Hui Xia, ZhipingJia, Lei Ju, Xin Li, Edwin H.-M. Sha, “Impact of trust modeled on-demand multi-path routing in mobile ad-hoc networks” published in science direct 2013, pp.1078–1093.

[8]Rahman A. A., and HailesS. “A Distributed Trust Model." Proceedings of the ACM New Security Paradigms Workshop, 1997, pp. 48-60

[9]Z. J. Haas and L. Zhou, “Securing Ad-Hoc Networks” IEEE Network Magazine, 13(6), 1999.

[10]N Li, JC Mitchell, W Winsborough, “Design of a role-based trust management framework," in Proceedings of the 2002 IEEE Symposium on Security and Privacy (May 2002), pp.58-73

[11]Q Memon, S Akhtar, AA Aly, “Role management in ad-hoc networks," in Proceedings of the 10th Communications and Networking Simulation Symposium (SCS and ACM, March 2007), pp. 131–137.

[12]Rehan Akbani and TurgayKorkmaz “Enhancing role-based trust management with a reputation system for MANETs” published in Akbani and Korkmaz; licensee Springer 2011

[13]Luo, J.H., Fan, M.Y.: ‘A subjective trust management model based on a certainty-factor for MANETs’, Chin. J. Comput. Res. Dev., 2010, 47, (3), pp. 515–523.

[14]Wenjia Li, Anupam Joshi, TimFinin “SMART: An SVM-based Misbehavior Detection and Trust Management Framework for Mobile Ad hoc Networks."

[15]Sonja Buchegger, JeanYves Le Boudec, “Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks)”, Networks)," ACM 158113501, June-2002.

[16]Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, “Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog” published in IEEE COMMUNICATIONS LETTERS, VOL. 16, NO. 5, MAY 2012, pp. 642-645.

[17]S. Marti, T.J. Giuli, K. Lai, M. Baker, “Mitigating routing misbehavior in mobile ad-hoc networks," Mobile Computing and Networking (2000), pp. 255–265.

[18]S. Ghazizadeh, O. Ilghami, E. Sirin, “Security-Aware adaptive Dynamic Source Routing Protocol," Proceedings of 27th Annual IEEE International Conference on Local Computer Networks, November 2002.

[19]Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu, " Trust Model Based Routing Protocol for Secure Ad-hoc Networks", published in IEEE 2004, pp.1-10

[20] YIH-CHUN HU∗ and ADRIAN PERRIG “Ariadne: A Secure On-Demand Routing Protocol for Ad -hoc Networks," published Springer 2005, pp.21-38.

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

[22]Islam Tharwat A. Halim 1, Hossam M. A. Fahmy 2, Ayman M. Bahaa El-Din 3, Mohamed H. El-Shafey 4,” Agent-based Trusted On-Demand Routing Protocol for Mobile Ad-hoc Networks” published in Fourth International Conference on Network and System Security, 2010, pp.255-262.

[23]H. Xia1 Z. Jia1 L. Ju1 Y. Zhu2 “Trust management model for mobile ad-hoc network based on analytic hierarchy process and fuzzy theory” Published in IET Wireless Sensor Systems, Vol. 1, Iss. 4, 2011, pp. 248–266

[24]Hui Xia, Zhipingjia, Xin Li, Lei ju,“Trust Prediction and Trust-based source routing in mobile ad-hoc networks” , Computer Communications 2012, pp. 2096–2114

[25]B. Scholkopf, and A. J. Smola, “Learning with Kernels," The MIT Press, pp.204-205, 2006.

[26] Meenakshi Patel, Sanjay Sharma, “Detection of Malicious Attack in MANET A Behavioral Approach," published in IEEE 2012, pp.388-393.

[27] Vijay Kumar Singh, Piyush Kumar Shukla, Sachin Goyal, “Survey of Various Trusts Based QoS Aware Routing Protocol in MANET,” GJRA -

GLOBAL JOURNAL FOR RESEARCH ANALYSIS, Volume-5, Issue-11, November – 2016, pp. 468-470, ISSN No. pp. 2277 – 8160.

[28] Vijay Kumar Singh, Piyush Kumar Shukla, Sachin Goyal, " Dispersed Opinion based QoS Cognizant Routing Protocol against Black hole Attack in MANET, " *IOSR Journal of Mobile Computing & Application (IOSR-JMCA) e-ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 3, Issue 6 (Nov. - Dec. 2016), PP. 29-37* www.iosrjournals.org.