Volume 6, Issue 6, June 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Trust Based Mobile Ad-hoc Networks

Ranjana Sharma
M.Tech, SSGI, KUK University,
Haryana, India

Anuradha Panjeta
Assistant Professor (CSE), SSGI, KUK University,
Haryana, India

Abstract—This paper mainly focused upon the architecture, history, types of Attacks, comparative analysis of previous techniques already found. In this paper, just a brief introduction is given on MANET, few routing protocols, Trust and trust management with a Trust based Routing Protocol to mitigate the effect of various attacks like Black hole effect etc that occurs due to dynamic behaviour or malicious nodes with the communication process.

Keywords— Mobile Ad hoc Network, Security, Trust, Routing, Attacks, Reputation

I. INTRODUCTION

MANET (Mobile Ad-hoc Network) is a popular and widely used wireless network. MANET is a kind of self-organizing and decentralized system. It is a network made up of various wireless mobile nodes which collectively work together so that transmission is feasible between any of the nodes in the system. [2]Nodes communicate with each other with the direct shared wireless radio links.[4] All the mobile hosts act as routers in the network. Due to open and dynamic nature, this network is quite prone to number of attacks. Information in the form of packets is transmitted from source to destination with the help of other nodes in the route. [1]There are certain things which should be noticed as Route selection, Request initiation, topology used etc.

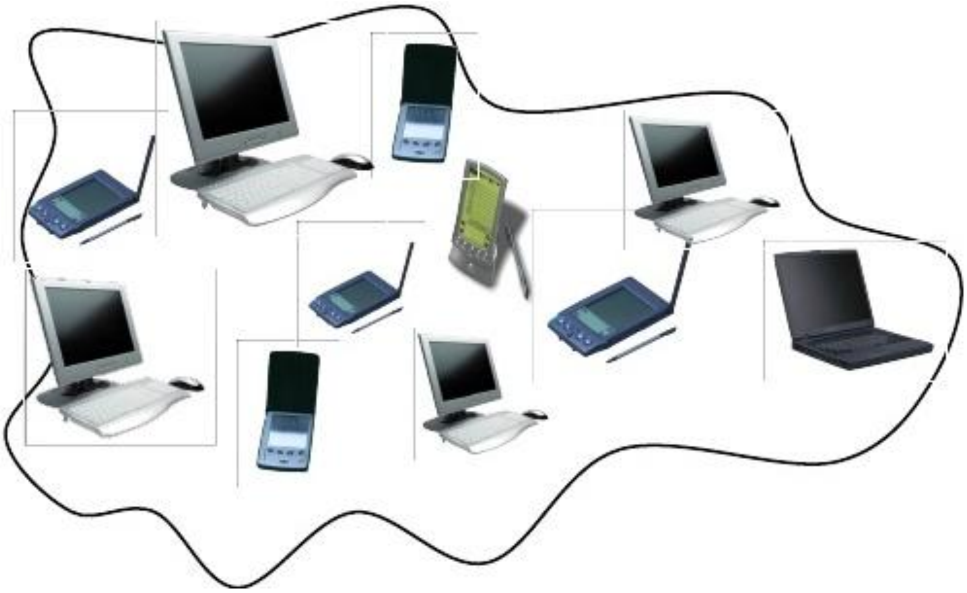

Fig 1. Architecture of Mobile Ad-hoc network

The routing scheme in MANET is more challenging than traditional networks. To handle the network with large number of hosts, many routing protocols like AODV, DSR with limited resources like energy and bandwidth but no security consideration have been made. Further many secure routing protocols are developed to secure the network.

Trust is defined as a degree of belief among various entities. The trust for same entity can be different when evaluated by different people. Trust management is a system that will assure various important features like security, access control, intrusion detection, isolating malicious nodes etc.

During communication, a selfish node to save its resource, does not cooperate and even drops the packet. To avoid this, reputation mechanisms are used. A reputation is defined as an import of the past behavior of an entity. The reputation system maintains a blacklist which contains the records of malicious nodes. Malicious nodes cause various attacks like Black hole attack and cooperative black hole for which a Trust based approach is used. In this trust value associated with each node which is represented with the trustworthiness to each of its neighboring nodes is calculated.

The Paper is structured as follows: History of MANET is discussed in section II, Types of Attacks in MANET is presented in section III, Literature Survey is explained in section IV , Conclusion is written under section V and in the end References is given.

II. HISTORY OF MANET

In 1970, MANET was known as “Packet Radio Network” earliest, sponsored by DARPA (Defence Advance Research Project Agency). In 1980, DARPA experiments included the survivable Radio Networks Project. The advent of inexpensive 802.11 radio cards for personal computers in 1990 spread it all over. Now, MANET is mainly used in military purposes.

III. VARIOUS TYPES OF ATTACKS

Denial of service attacks:- It focuses at complete disruption of routing information and therefore the whole operation of ad-hoc network.

Snooping:- Snooping is unauthorized access to another person's data. To remotely monitor activities on a computer or network device many sophisticated snooping software programs are used.

Flooding attack:- In this attacker damages the network resources, such as bandwidth and to consume a node’s resources, such as computational and battery power or to cause severe degradation in network performance.

Rushing attack:- Basically it is against on-demand routing protocols. It actually ruins the route discovery process.

BlackHole attack:- A severe attack that can be easily signed against data routing in MANETs. In this a malicious node drops all the receiving data packets and returns erroneous reply for any route requests without having an actual route to a specified destination. [6]

Colluding misrerlay attack:- In this, multiple attackers work in scheme to not only modify but also drop routing packets to distrub routing operation in a MANET.

Gray-hole attack:- It is a special case of black hole attack where the data packets are selectively dropped. [7]

IV. LITERATURE SURVEY

POONAM, K. GARG et al. (2010) Ad-hoc networks establish communication in improvised environments without requiring any rigid infrastructure. These networks are inherently supine to security attacks, with node mobility being the major source in allowing security breaches. Therefore secure routing is a must for such networks. In this paper, the author presented a unique trust based method which is not vulnerable to this behaviour. In this method, if a node receives a RREQ packet from different neighbours it broadcast it to other nodes. The weighted average of the trustvalue of the nodes, with respect to its behavior observed by its neighboring nodes and the number of nodes in the route is a secure and efficient route to the destination. The author calculated the misbehaving node detection rate and the efficiency of his method along a number of parameters. Results show that his method increases the throughput of the network while discovering a secure route.[2]

SHEN MING-YU et al. (2010) this paper published by the author describes the Authentication Test Theory of strand space firstly and expended because of the demands of mobile ad hoc network routing protocol security analysis. Based on Ariadne routing protocol, a new Ariadne-S protocol model is proposed by analyzing the existing security Dynamic Source Routing routing protocol. Then it is proved that the concluding routing information from the technique of routing finding are efficient and credible by using strand space model.[3]

R. SUDHA et al. (2011) several routing protocols have been proposed for MANETs and prominent among them are DSR, AODV and TORA. However, these routing protocols did not provide a complete solution for all the attacks and assumed that any node involved in the MANET is not hoggish and that it will help to collaborate different network functionalities. One of the feasible solution to the security problem is ARAN –(Authenticated routing protocol) which is a secure protocol and facilitates features like Integrity, availability, Confidentiality, Authenticity, Non repudiation, Authorization & Anonymity but a selfish node can disturb protocol’s performance and even the network by dropping packets. This paper also discusses Temporal table based schemes that can be subjected to ARAN for figuring out selfish node and thus improve the performance.[4]

RAMASAMY MARIAPPAN et al. (2011**)** in this paper, the author presented new protocol design scenario like Re - Pro Routing Protocol for Broadcasting in wireless MANET and a comparative performance for MANET protocols like as Ad-hoc On-Demand Distance Vector Routing protocol spotlighting the effects of changes such as the rising number of receivers or sources and increasing the total number of nodes. A systematic performance interpretation of these protocols is carried out by performing simulations and the trust methods in mobile Ad-Hoc networks and these mechanisms are prone to security hazards but have found their approval due to efficiency over computationally expensive and tedious cryptographic methods. This paper also proposed security mechanism dependent upon Electronic Code (EC) combined with permutation functions.[5]

MEHDI KESHAVARZ et al. (2012) free-riding by packet dropping is one of the most important aspects for the establishment and sustainability of the open multi-hop wireless networks. In this paper, main focus is on the packet dropping in a dense MANET. To confront this situation, a scheme based on using MAC-layer acknowledgements to detect and punish packet dropper nodes is invented. The author used simulation-based (using NS-2) results to evaluate the performance of scheme.[8]

ISAAC WOUNGANG et al. (2012) from a security design perspective, MANETs have no clear line of defence; i.e. no built-in security. Thus, the wireless channel is available to both consistent network users and malicious attackers. A novel theory for searching Blackhole Attacks in MANETs (so-called DBA-DSR) is made. The BDA-DSR protocol not only detects but also dodge the blackhole problem before the actual routing mechanism begins by using fictitious RREQ packets for the acquisition of malicious nodes.[6]

MOHAMMED S. OBAIDAT et al. (2012) securing the routing of message in mobile ad hoc networks (MANETs) is still a major concern. In this paper, the author proposes an Enhanced Trust based Multipath Dynamic Source Routing Protocol for transmitting Message with security. The author's method consists in a combination of soft-encryption, novel trust management scheme, and multipath DSR routing. [9].

R. MENAKA et al. (2013) collaboration and Cooperation is quite difficult in managing trust in a distributed MANET. This is also severe in obtaining system aims like reliability, availability etc. This paper discusses concept and features of trust and provides an analysis of trust management schemes in MANET. The accepted classifications, potential attacks, and trust metrics are discussed. [7]

NILESH N. DANGARE et al. (2015) as its open, dynamic behavior, MANET is highly prone to various attacks. Various existing system for detection of attacks is in-competent and may require more processing and space as in cryptography techniques. In this Paper, the focus is given on the trust based approach to eliminate the intrusion in Trust Based Approach, instead of shortest path, the most trusted path is selected [1]

ALGORITHMS	AUTHOR & YEAR	FEATURES	FINDINGS
Trust-embedded AODV (T-AODV) routing protocol from independent malicious nodes by finding a secure end-to-end route	Poonam, k. garg & M Misha in 2010	This method increases the throughput of the network while discovering a secure route.	A secure and competency path to the destination is calculated as a weighted average of the trust value of the nodes, with respect to its behaviour examined by its neighbouring nodes and the number of nodes in the route.
DSR routing protocol	SHEN Ming-yu & LI Cang-yuan in 2010	Proved that the returning routing information from the process of routing finding is secure and credible by using strand space model.	By analyzing the existing security DSR routing protocol leaks, a new Ariadne-S protocol model is recommended based on Ariadne routing protocol.
ARAN – (Authenticated Routing Protocol)	R. Sudha & Dr. D. Sivakumar in 2011	For Network security a solution – ARAN is given. which is a secure protocol and provides Integrity, availability etc.	This paper discusses Temporal table based schemes that can be practised to ARAN to investigate selfish node and thus to improve the overall performance.
Re- Pro Routing Protocol (RPRP)	Ramasamy Mariappan & Sangameswaran Mohan in 2011	The result is a network with less overhead, at the expense of increased latency.	This paper proposes security mechanism dependent upon Electronic Code (EC) combined with permutation functions.
MAC-layer acknowledgements	Mehdi Keshavarz & Mehdi Dehghan in 2012	In this paper, basic focus on the data packet dropping in a rather condensed MANET. To encounter this situation, the author proposed a theory based on using MAC-layer acknowledgements to find and punish packet dropper nodes.	The author used using NS-2 simulation-based results to evaluate the performance of our scheme.
DBA-DSR scheme	Isaac Woungang , Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi & Mohammad S. Obaidat in 2012	Before starting actual routing mechanism, The BDA-DSR protocol detects and avoids the blackhole problem by using fake RREQ packets to catch the malicious nodes.	A novel scheme for identifying Blackhole Attacks in MANETs (so-called DBA-DSR) is introduced.
Trust-Based Multipath DSR message Scheme	Mohammed S. Obaidat & Han-Chieh Chao, Chris Liu In 2012	Simulation results are presented to validate tender, showing that ETB-MDSR scheme surpasses a recently proposed Trust-Based Multipath DSR message scheme (TB-MDSR), for route selection time.	This paper proposes an Enhanced trust-based multipath Dynamic Source Routing (DSR) protocol to securely transmit messages in MANETs.
Trust enhancement	R. Menaka & Dr. V. Ranganathan in 2013	This is also critical in achieving mission and system aims like reliability, availability, scalability, or reconfigurability.	With concepts and properties of trust , this paper focuses in providing a survey of MANET developed trust management schemes.
Trust based Approach	Nilesh N. Dangare & R. S. Mangrulkar in 2015	In Trust based approach, instead of shortest path, the most trusted path is selected.	To mitigate the attack, The focus is given on the Trust based approach.

V. CONCLUSION

We conclude that Trust-embedded AODV is used to calculate a secure and efficient route to the destination with increased throughput of a network. A new Ariadne-S protocol model proved that the returning routing information from the process of routing finding is secure. Temporal table based schemes can be applied to ARAN (Authenticated Routing Protocol) to detect selfish node and improve the performance. Re- ro Routing Protocol is a security mechanism dependent upon Electronic Code combined with permutation functions which returns a network with less overhead. A scheme based on using MAC-layer acknowledgements is used to detect and punish packet dropper nodes. Before starting the actual routing mechanism, BDA-DSR protocol not only detects but also avoids the blackhole problem. Enhanced trust-based multipath DSR protocol is used to securely transmit messages in MANETs. Trust enhancement schemes are used to achieve reliability, scalability etc. Trust based Approach is used to selected the trusted path which will mitigate the various attacks.

REFERENCES

[1] Nilesh N. Dangare M. Tech. (CSE) BDCOE, R. S. Mangrulkar Associate Professor Head Comp. Engg, BDCE, “Design and Development of Trust Based Approach to Mitigate Various Attacks in Mobile Ad-hoc Network”, International Journal of Computer Applications (0975 – 8887) International Conference on Quality Up-gradation in Engineering, Science and Technology (ICQUEST2015).

[2] Poonam, K. Garg, M. Misra, Indian Institute of Technology Roorkee, India “Trust Based Multi Path DSR Protocol”, 2010 International Conference on Availability, Reliability and Security.

[3] SHEN Ming-yu, LI Cang-yuan, School of Computer & Information. Hefei University of Technology Hefei, China, “Research and Analysis On Secure DSR Routing Protocol Based on Strand Space”, 2010 International Conference on Electrical and Control Engineering.

[4] R. Sudha, S.Lecturer, CSE, Dr.Pauls Engineering College. Villupuram, Dr. D. Sivakumar, Professor & Head Department of IT, Adhiparasakthi Engineering College. Melmaruvathur, “A Temporal table Authenticated Routing Protocol for Adhoc Networks”, 978-1-4577-1894-6/11/$26.00©2011 IEEE.

[5] Ramasamy Mariappan Sangameswaran Mohan Professor, Department of CSE Department of CSE Adhiparasakthi Engineering College, Melmaruvathur, “Re-Pro Routing Protocol with Trust Based Security for Broadcasting in Mobile Ad hoc Network”,978-1-4673-0671-3/11/$26.00©2011 IEEE.

[6] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, Mohammad S. Obaidat, “Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks”, 978-1-4673-1550-0/12/$31.00 ©2012 IEEE.

[7] R. Menaka, Dr. V. Ranganathan, “A Survey of Trust related Routing Protocols for Mobile Ad Hoc Networks” International Journal of Emerging Technology and Advanced Engineering,ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013.

[8] Mehdi Keshavarz, Mehdi Dehghan, "MAC-Aided Packet-Dropper Detection in Multi-Hop Wireless Networks" 978-1-4673-0682-9/12/$31.00 ©2012 IEEE.

[9] Isaac Woungang, Mohammed S. Obaidat, Sanjay Kumar Dhurandher, Han-Chieh Chao, Chris Liu, "Trust-Enhanced Message Security Protocol for Mobile Ad Hoc Networks" 978-1-4577-2053-6/12/$31.00 ©2012 IEEE.