IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. II (May – Jun. 2015), PP 01-05
www.iosrjournals.org

Routing and Security Issues for Trust Based Framework in Mobile Ad Hoc Networks

Mukesh Kumar Garg[1], Neeta Singh[2]
[1]*(Department of Computer Engineering, YMCA University of Science & Technology, Faridabad, Haryana, India)*
[2]*(Department of Computer Science and Engineering, School of I.C.T., Gautam Buddha University, Greater Noida, Uttar Pradesh, India)*

Abstract: *Mobile means moving and Ad Hoc means temporary without any fixed infrastructure, so mobile ad hoc networks (MANETs) are a kind of temporary networks in which nodes are moving without any fixed infrastructure or centralized administration. It is the new emerging technology which enables user to communicate without any physical infrastructure regardless of their geographical location, that's why it is also referred to as an "infrastructure less" network. Unfortunately, ad hoc networks are particularly vulnerable due mainly to their lack of infrastructure. Other reasons could be: high mobility, wireless links, limited bandwidths, lack of boundaries, short lifetime batteries and weak capacity of equipments. The execution and survival of ad hoc networks depends on cooperative and trusting nature of the distributed nodes. There is a common assumption in the routing protocols that all nodes are trustworthy and cooperative. However, this naïve dependency on intermediate nodes makes the ad hoc networks vulnerable to passive and active attacks by malicious nodes. Trust based routing and Security in MANETs are the most important concern for the basic functionality of Network. The availability of network services, confidentiality and integrity of data can be achieved by assuring that routing & security issues have been met. In this paper an attempt has been made to review various routing and security issues for trust based framework in MANETs.*

Keywords: *MANETs, Routing Issues, Trust, Security Issues.*

I. Introduction

MANETs have received significant research attention since the development of packet radio networks in the 1970s. MANETs [1-4] are wireless networks that continually re-organize themselves in response to their environment without the benefit of a pre-existing infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. A fundamental characteristic of MANETs is that they are able to configure themselves on-the-fly without the involvement of a centralized administrator. Although all wireless networks as shown in Fig. 1 work without any physical connection but with a fixed infrastructure. The increasing use of wireless portable devices such as mobile phones and laptops as part of everyday life, is leading to the possibility for unstructured or ad hoc wireless communication. With these types of devices, there is a fundamental ability to share information. There is no need of access points, each node act as a router and node at the same time. These mobile nodes (router) can leave and join the network according to their own wish. Every node finds the route-by-route request.

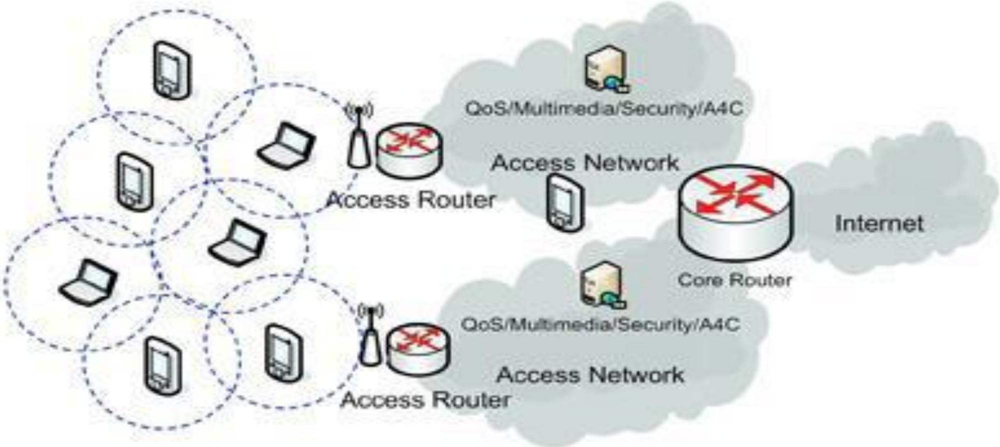

Fig. 1 An example of various Wireless Networks

Routing is a mechanism, which is used to find the path between the source to the destination among randomly distributed nodes. Routing protocol plays an important role to send the data from source to destination that discovers the optimal path between the two communication nodes [5]. Every protocol has its own rules to finds the route or maintenance the route. There are various routing protocol proposed by researchers. These are broadly divided into three categories (based on the Routing Information Update Mechanism) [1], [3]: Proactive (table-driven), Reactive (source-initiated on-demand-driven) and Hybrid. The proactive protocols maintain routing information about each node in the network. The information is updated throughout the network periodically or when topology changes. Each node requires to store their routing information. For example: Bellman-Ford Routing Protocol, Destination Sequenced Distance Vector Routing (DSDV), Source Tree Adaptive Routing (STAR). The reactive routing protocols look for the routes and are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. For example: Ad-Hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), Dynamic MANET On-demand (DYMO). The hybrid routing protocols are using the best features of both the on-demand and table driven routing protocols. For example: Temporally Ordered Routing Algorithm (TORA), Zone Routing Protocol (ZRP).

Since nodes in MANETs can move arbitrarily the topology may change frequently at unpredictable times. Transmission and reception parameters may also impact the topology. So it is very difficult to find and maintain an optimal route taking trust as a parameter. The routing algorithm must react quickly to topological changes as per the degree of trust of a node or a complete path between a source and a destination pair. Nodes in MANETs communicate over wireless links. Therefore efficient calculation of trust is a major issue in MANETs because an ad hoc network depends on cooperative and trusting nature of its nodes. Although the security requirements are different from one application to another, they are not negligible in most cases. To enhance security in ad hoc networks, it is important to evaluate the trustworthiness of other nodes without central authorities. A considerable amount of work has been done on trust based routing. Yet there are some issues which are not addressed clearly in the existing papers. These issues are like concept of malicious node/selfish node, calculation of trust, concept of central trust authority, proactive nature of calculation and lack of security model for cryptographic analysis of trust based routing. If these issues may be taken care of then an efficient and robust trust based protocol can be developed. Trust based routing and Security in MANETs are the most important concern for the basic functionality of Network. The availability of network services, confidentiality and integrity of data can be achieved by assuring that routing & security issues have been met. The highly dynamic nature of MANETs coupled with limited bandwidth and battery power imposes severe restrictions on routing protocols especially on achieving the routing stability. Due to all these constraints, designing of a routing protocol is still a challenging task for researchers. As the nodes are dynamic the number of nodes in route selection is always changing thus the degree of also keep changing. There are some issues in MANETs regarding trust based routing which are not being mentioned clearly in the existing trust based routing proposals [5-11], [22-26].

In this paper an attempt has been made to review various routing and security issues for trust based framework in MANETs. Some of these issues are pointed out in this paper in Section 2. The rest of the paper is organized as follows: Section 3 presents security, security goals, security attacks on ad hoc networks and secure routing for MANETs. Section 4 describes the concept of trust, trust establishment and some issues related to trust based routing in MANETs. Finally, Section 5 gives the conclusion which includes the highlights of trust based system and future work.

II. Problem Formulation and Major Issues

The key issue with ad-hoc networking is how to send a message from one node to another with no direct link. The nodes in the network are moving around randomly, and it is very difficult that which nodes are directly linked together and the intermediate node judges its ability to forward the RREQ packets or drop it [12]. The number of packets transferred successfully by each node. Route from source to destination is determined by selecting the most trusted path [13]. Here battery capacity is not considered as an issue for selecting the path between source and destination. Same time topology of the network is constantly changing and it is very difficult for routing process. We efforts to simulate and analyze of these two parameters to discover a reliable route between the source and destination and reduce power consumption. Trust is extracted from social relationship. It is always established between two parties for a specific action. In particular, one party trusts the other party to perform an action. Trust may be referred as belief or reputation of one entity to other to perform an action [14]. Trust in entities is based on the fact that the trusted entity will not act maliciously in a particular situation. As no one can ever be absolutely sure of this fact, trust is solely dependent on the belief of the trustor. Trust may be calculated directly or indirectly depending upon the nature of the protocol. While in most of the proposals it is calculated indirectly with the use certification method. In this case no direct trust can be established between two nodes rather nodes become dependent of the previous calculations of other neighbouring nodes. Different metrics can be used for trust like belief, reputation, linguistic descriptions in [15], discrete integers in [16], continuous value in [0,1] in [17], a 2-tuple in [0,1]2 in [18], and a triplet in [0,1]3 in [19].

III. Security in Ad Hoc Network

The research on wireless ad hoc network indicates that security is a major issue providing protected communication between mobile nodes in a hostile environment. Owing to the challenges posed by inherent characteristics of MANETs, the existing security mechanisms of wired networks cannot be applied to MANETs. The challenges being include wireless medium, highly dynamic topology, distributed cooperation, resource-constrained capability, and limited physical security. In fact, these challenges necessitate the building multifence security solutions that achieve both broad protection and desirable network performance.

3.1 Security Goals

Every routing protocol needs secure transmission of data. Security service requirements of MANETs are similar to wired or any infrastructure wireless network. Following are major security goals which are needed for protecting the data and resources from attacks:

i) Authentication ensures that the communication or transmission of data is done only by the authorized nodes. Without authentication any malicious node can pretend to be a trusted node in the network and can adversely affect the data transfer between the nodes.

ii) Availability ensures the survivability of the services even in the presence of the attacks. Availability is concerned with the fact that the network services should be available whenever they are needed. Systems ensuring the availability in MANET's should be able to take care of various attacks such as denial of services, energy starvation attacks, and node misbehavior.

iii) Confidentiality ensures that information should be accessible only to the intended party. No other node except sender and receiver node can read the information. This can be possible through data encryption techniques.

iv) Integrity ensures that the transmitted data is not being modified by any other malicious node. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.

v) Non-Repudiation ensures that neither a sender nor a receiver can deny a transmitted message. Non-repudiation helps in detection and isolation of compromised node.

vi) Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

vii) Authorization assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

3.2 Security Attacks on MANETs

In Infrastructure less networks there is much more need for the security as each node is free to move in any direction and there is no centralized security provision in such networks which implies the identification of potential attacks, threats and vulnerability of a certain system. The security attacks on MANET's are broadly divided into two major categories:

i) Active Attacks: Those attacks which try to interrupt the proper functionality of the network. This can be done either through reading and changing the information on the data packets, denial of Services, altering the routing path by changing routing information, hop count etc. These attacks are easier to be detected as compare to their counterpart i.e. Passive attacks. For e.g.:

○ MAC layer attacks: Jamming
○ Network layer attacks: Black hole, Gray hole, Worm hole etc.
○ Transport layer attacks: Session hijacking
○ Application layer attacks: Repudiation

ii) Passive Attacks: Those attacks which do not alter the normal functionality of network but silently try to listen or retrieve the vital information inside the data packets. These kinds of attacks are hard to detect. For e.g.:

○ Snooping, Selfishness

3.3 Secure Routing for MANETs

Security protocols for MANETs can be mainly categorized in two major categories:

i) Prevention: This mechanism involves protocols which prohibit the attacking node to initiate any action. This approach requires encryption technique to authenticate the confidentiality, integrity, non-repudiation of routing packet information.

ii) Detection and Reaction: Detection and Reaction mechanism as the name suggest will identify any malicious node or activity in the network and take proper action to maintain the proper routing in the network.

IV. Trust in Ad Hoc Networks

The execution and survival of an ad hoc network is solely dependent upon the cooperative and trusting nature of its nodes. Trust and security are two tightly interdependent concepts that cannot be desegregated. For example, cryptography is mean to implement security but it is highly dependent on trusted key exchange. Similarly, trusted key exchange cannot take place without requisite security services in place. It is because of this inter-reliance that both these terms are used interchangeably when defining a secure system. The term trust can be defined as:

Trust is the degree of belief about the future behaviour of other entities, which is based on the ones the past experience with and observation of the other's actions. In other words it can define as the trust is always established between the two parties for a specific action. In particular, one party trusts the other party to perform the action.

Trust is also time dependent, it grows and decays over a period of time. A pure ad-hoc network closely resembles this human behaviour, where a number of people/nodes that have never met each other, are able to communicate with each other based on mutual trust levels developed over a period of time.

Trust establishment in wired networks is usually achieved using indirect trust mechanisms, including trusted certification agencies and authentication servers. However, establishing this indirect trust still requires some out-of-band mechanism for initial authentication and is usually dealt with physical or location-based authentication schemes.

Trust establishment in ad-hoc wireless networks is still an open and challenging field.

4.1 Trust Establishment in Ad Hoc Networks

Trust has been established in ad-hoc networks using a number of assumptions including:

- Pre-configuration of nodes with secret keys.
- Presence of an omnipresent central trust authority.
- Mutual trust levels developed over a period of time.

4.2 Trust Issues and Requirements

There are some issues in mobile ad hoc networks regarding trust based routing which are not being mentioned clearly in the existing trust based routing proposals [5-11]. Some of these issues are pointed out in this section as follows:

i) Malicious/Selfish Node: Definition of a malicious/selfish node is come into existence in [20] Whenever a node receives a request to relay traffic, it normally perform an action on the request while practically, intermediate node may not wish to consume their energy to carry some other node's traffic. This is known as selfish behaviour of a node and that node is referred as a selfish node. In the similar fashion if a large number of nodes behave selfishly and refuse to act as an intermediate node between a pair of source and destination, network efficiency will be reduced upto a great extent. Although a definition of malicious node is given here but yet none of the existing definition of malicious node in the existing proposals defines the reason or ground rules for marking a node as malicious or selfish node. In other words none of the previous work identifies that why a node is not interested in forwarding the relay traffic between a source-destination pair. So there is a need to introduce some ground rules or a set of all possible reasons due to which a node may be considered as malicious or selfish node.

ii) Definition and Calculation of Trust: In case of trust again there are confusions in the definition of trust because in wired networks whether a node is reliable or not is identified by certification mechanism which is an indirect method of trust calculation. On this basis reliability and non-maliciousness can be clubbed together. While marking a node as malicious or no reliable in MANETs is not easy due to dynamic changing topology. It is very difficult to incorporate certification mechanism in ad hoc networks, because reliability and maliciousness has to be taken care as separate issues. In wireless network reliability/security is a global issue while trust is a local issue of the routing and as in the existing trust based routing proposal authors have given a trust based model without specifying a security analysis of the proposed model against attacks. Therefore there is need to develop a trust based model considering security as an important parameter. Calculation of trust for an individual node or a path is done in several papers [5-11], [21]. But it is not mentioned clearly in any of the referenced paper that how nodes can calculate and advertise the trust among the network. Although a detailed method is presented in [21] but again calculation of advertise trust is not clearly mentioned.

iii) Proactive Nature of Trust based Protocols: All the existing work shows that dynamic computation of trust is proactive in nature and contain a lot of overheads due to access use of control packets which are used for advertising trust, calculating observed trust and issuing certificates in the trust calculation. This overhead is due to the indirect calculation of trust of a node or a path. Therefore direct trust mechanism is required instead of recommendation from trusted third party.

V. Conclusion and Future Work

In this paper some of the challenges of MANETs are discussed in term of routing & security issues. There are also requirement of changes related to trust based routing has been pointed out. These issues are supposed to take good care for developing an efficient, secure and robust routing protocol for wireless ad hoc networks. Taking these issues in to account handling and identification of malicious node can be done easily as well as a model can be developed for calculating trust and analyzing security of the model.

Acknowledgements

The authors wish to acknowledge Dr. Ela Kumar, Professor and Dean Academic Affairs, Department of Computer Science & Engineering, Indira Gandhi Delhi Technical University for Women, Kashmere Gate, Delhi, India, for her continual support to carry out this work. The authors also wish to acknowledge YMCA University of Science & Technology, Faridabad, Haryana, India, for its continual support to carry out this work.

References

[1]. C. Siva Ram Murthy and B. S. Manoj, “Ad Hoc Wireless Net-works, Architecture and Protocols,” Pearson Education, Fourth Impression, 2009.

[2]. M. Abolhasan, T. Wysocki and E. Dutkiewicz, “A review of Routing Protocols for Mobile Ad Hoc Networks”, Ad Hoc Networks, Vol. 2, Issue 1, PP. 122, Jan. 2004.

[3]. Elizabeth M. Royer and Chai-Keong Toh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”, IEEE Personal Communications Magazine, Vol. 6, No. 2, PP. 46-55, April 1999.

[4]. Scott Corson and Joseph Macker, “Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, IETF MANET, RFC 2501, 1999.

[5]. Huafeng Wu1, Chaojian Shi1,” A Trust Management Model for P2P File Sharing System”, International Conference on Multimedia and Ubiquitous Engineering, IEEE Explore 978-0-7695-3134-2/08, 2008.

[6]. Z. Ye., S. V. Krishnamurthy and S. K. Tripathi, “A Framework for Reliable Routing in Mobile Ad Hoc Networks”. In the Proceedings of 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM) 2003, 270-280.

[7]. X. Li, M. R. Lyu, J. Liu, “A Trust Model Based Routing Protocol for Secure Ad Hoc Networks”. In the Proceedings of IEEE Aerospace Conference (IEEEAC), 6-13 March 2004, Vol. 2, 1286-1295.

[8]. M. Virendra, M. Jadliwala, M. Chandrasekaran, S. Upadhyaya, “Quantifying Trust in Ad-Hoc Networks”. In the Proceedings of IEEE international Conference on Integration of Knowledge Intensive Multi Agent systems (KIMAS) 2005, 65-71.

[9]. Z. Liu, A. W. Joy and R. A. Thompson, “A Dynamic Trust Model for Mobile Ad Hoc Networks”. In the Proceedings of 10th IEEE international workshop on Future Trends of Distributed Computing Systems (FTDCS), 28 May 2004, 80-85.

[10]. L. Eschenuer, V. D. Gligor, J. Baras, “On Trust Establishment in Mobile Ad-Hoc Networks”. Security Protocols: 10th International Workshop, 2002, 47-62.

[11]. Asad Amir Pirzada and Chris McDonald, “Establishing Trust in Pure Ad-hoc Networks”. In the Proceedings of the 27th Australasian Conference on Computer Science, Vol. 26, PP. 47-54, 2004.

[12]. P. Sinha, R. Sivakumar, and V. Bharghavan, “CEDAR: A Core Extraction Distributed Ad-hoc Routing Algorithm”. IEEE Journal on Selected Areas in Communications,Vol. 17, No. 8, pp. 1454-1466, 1999.

[13]. M. Tamilarasi, T. G Palani Velu, “Integrated Energy-Aware Mechanism for MANETs using On-demand Routing”, International Journal of Computer, Information and Systems Science and Engineering 2; www.waset.org Summer 2008.

[14]. D. H. McKnight and N. L. Chervany, “The meanings of Trust,” MISRC Working Paper Series, Technical Report 94-04, Arlson School of Management, University of Minnesota, 1996.

[15]. M. Blaze, J. Feigenbaum, and J. Lacy, “Decentralized Trust Management,” In Proceedings of the 1996 IEEE Symposium on Security and Privacy, PP. 164-173, May 1996.

[16]. A. A. Rahman and S. Hailes, “A Distributed Trust Model”. In the Proceedings of the ACM workshop on New Security Paradigms 1998, 48-60.

[17]. U. Maurer, “Modeling a public-key infrastructure,” In Proceedings 1996 European Symposium on Research in Computer Security (ESORICS’ 96), Volume 1146 of Lecture Notes in Computer Science, PP. 325-350, 1996.

[18]. G. Theodorakopoulos and J. S. Baras, “Trust Evaluation in Ad-Hoc Networks,” In Proceedings of the ACM Workshop on Wireless Security (WiSE’04), Oct. 2004.

[19]. A. Jsang, “An Algebra for Assessing Trust in Certification Chains,” In Proceedings of the Network and Distributed Systems Security (NDSS’99) Symposium,1999.

[20]. Vikram Srinivasan, Pavan Nuggehalli, Ramesh R. Rao, “Energy Efficiency of Ad Hoc Networks with Selfish Users”, San Jose, California, Mobicom-01. 2002.

[21]. Kamal Deep Mekaetal, “Trust Based Routing Decisions in Mobile Ad Hoc Networks,” In Proceedings of The Second Secure Knowledge Management Workshop (SKM), 2006, National Science Foundation and the Polytechnic University, Brooklyn, NY.

[22]. A. Rajaram and Dr. S. Palaniswami, “The Trust-Based MAC-Layer Security Protocol for Mobile Ad hoc Networks”, International Journal on Computer Science and Engineering (IJCSE), Vol. 02, No. 02, 400-408, 2010.

[23]. Parul Tomar, Prof. P. K. Suri and Dr. M. K. Soni, “A Comparative Study for Secure Routing in MANET”, International Journal of Computer Applications, Volume 4 - No. 5, PP. 17-22, July 2010.

[24]. Sudhir Agrawal, Sanjeev Jain and Sanjeev Sharma, “A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks”, Journal of Computing, Vol. 3, Issue 1, January 2011.

[25]. Priyanka Goyal, Vinti Parmar and Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application”, International Journal of Computational Engineering & Management (IJCEM), Vol. 11, 32-37, January 2011.

[26]. Manisha and Dr. Mukesh Kumar, “Implementation and Removal of Co-operative black hole and worm hole Attacks on MANET with DSR”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, Issue 12, PP. 4147-4151, December 2014.