

Routing Issues for Trust Based Framework in Mobile Ad Hoc Networks

Mukesh Kumar Garg, Dr. Ela Kumar

Abstract— 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. 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.

Index Terms— MANETs, Selfish Nodes, Trust.

I. INTRODUCTION

MANETs are the collection of wireless nodes that can dynamically form a network anytime and anywhere to exchange information without using any pre-existing infrastructure. The highly dynamic nature of MANET [1], [2] 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. This paper addresses the problem of trust based routing in Mobile ad hoc network. Since mobile nodes in Mobile ad hoc network 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 Mobile ad hoc network communicate over wireless links. Therefore efficient calculation of trust is a major issue in mobile ad hoc networks because an ad hoc network depends on cooperative and trusting nature of its nodes. 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 mobile ad hoc networks regarding trust based routing which are not being mentioned clearly in the existing trust based routing proposals [3-8]. Some of these issues are pointed out in this paper in section II.

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 [9]. 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 [10], discrete integers in [11], continuous value in $[0,1]$ in [12], a 2-tuple in $[0,1]^2$ in [13], and a triplet in $[0,1]^3$ in [14].

The rest of the paper is organized as follows: Section II describes issues and requirements. Finally we present the conclusion and future work in Section III.

II. ISSUES AND REQUIREMENTS

A. Malicious/ Selfish Node:

Definition of a malicious/selfish node is come into existence in [15] 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.

B. 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 [3-8], [16]. 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 [16] but again calculation of advertise trust is not clearly mentioned.

C. 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.

III. CONCLUSION AND FUTURE WORK

In this paper some of the routing issues and change requirement 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.

ACKNOWLEDGMENT

The authors wish to acknowledge YMCA University of Science & Technology, Faridabad, India, for its continual support to carry out this work.

REFERENCES

- [1] Joseph Macker and Scott Corson, "Mobile Ad Hoc Networks (MANETs)", <http://www.ietf.org/proceedings/01dec/183.htm>, December 2001.
- [2] M. Abolhasan, T. Wysocki and E. Dutkiewicz, "A review of Routing Protocols for Mobile Ad Hoc Networks", Ad Hoc Networks, vol.2, issue1, pp.122, Jan.2004.
- [3] 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.
- [4] 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) 2004, 1286-1295.
- [5] M. Virendra, M. Jadhwal, 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.
- [6] 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) 2004, 80-85.
- [7] L. Eschenauer, V. D. Gligor, J. Baras, "On Trust Establishment in Mobile Ad-Hoc Networks". Security Protocols: 10th International Workshop, 2002, 47-62.
- [8] A. A. Pizada and C. McDonald, "Establishing Trust in Pure Ad-hoc Networks". In the Proceedings of the 27th Australasian conference on Computer Science 2004, 47-54.
- [9] 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.
- [10] 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.
- [11] A. A. Rahman and S. Hailes, "A Distributed Trust Model". In the Proceedings of the ACM workshop on New Security Paradigms 1998, 48-60.
- [12] 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.
- [13] 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.
- [14] A. Jsang, "An Algebra for Assessing Trust in Certification Chains," in Proceedings of the Network and Distributed Systems Security (NDSS'99) Symposium, 1999.
- [15] Vikram Srinivasan, Pavan Nuggehalli, Ramesh R. Rao, "Energy Efficiency of Ad Hoc Networks with Selfish Users", San Jose, California, Mobicom-01.
- [16] 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.



Mukesh Kumar Garg – received M.Tech. degree in Computer Engineering from MD University, Rohtak, Haryana, India in the year 2010. He started his carrier as Field & Customer Support Engineer in the field of Computers and Networking since 1991. At present he is working with the Department of Computer Engineering, YMCA University of Science & Technology, Haryana, India. His research interests include Mobile Ad Hoc Networks and Software Testing.



Dr. Ela Kumar – received B.E. in Electronics & Communication and M.Tech. in Computer Science and Technology from IIT Roorkee, in 1988 and 1990, respectively. She received her Ph.D. degree in the area of Natural Language Processing from Delhi University in 2003. She is actively engaged in Technical teaching and research since last 23 years. She has published almost 58 research papers in International Journals, National Journals, International Conferences and National Conferences. She has authored four books and many course materials related to Computer Science. She has supervised four doctoral research candidates. She is on the reviewer panel of many international journals. She has been conferred Rashtriya Gaurav Award and her bibliography was included in Asian Admirable achiever 2011. Presently she is working as Dean, School of Information & Communication Technology, Gautam Budhha University, Greater Noida, UP, India. Her research interest includes Designing of Intelligent Systems, Natural Language Processing, Mobile Ad Hoc Networks and Search Engine Optimization.