ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Trust Management Model Observation towards Security Enhancements and QoS in MANET's

A.Jayakumari [1], M.Sakthivel[2]

Final Year MCA Student, VelTech HighTech Engineering College, Chennai, Tamil Nadu, India[1]

Assistant Professor, Department of MCA, VelTech HighTech Engineering College, Chennai, Tamil Nadu, India[2]

ABSTRACT: Mobile Ad Hoc Network (MANETs) is a group of mobile nodes connected with wireless links. MANET has topology as the nodes are moving constantly form one position to another position. All the nodes must co-operate with each other in order to route the packets. Cooperating nodes must trust each other. In defining and managing trust in a army MANET, Therefore trust is vital sound which affects the performance of MANET. There are several protocols proposed based on the trust. Mobile Adhoc Network distress from security vulnerabilities because of its dynamic topology and open wireless medium. So there is a chance for malicious node to participate in the routing procedure and leads to the packet lose. In this paper, we develop a trust management scheme which enhances the security issues in Mobile Adhoc Network In the trust management scheme with trust value for each node will evaluate. The trust value calculated from two types of observation one is direct and another is indirect. Combining these two values we get a most accurate trust value then we evaluate the scheme under the circumstances of routing. By this process we can improve the security in Mobile Adhoc Network and increase the packet delivery ratio. This paper is a study trust model based protocols and it proposes some new techniques on trust model management ,security enhancement and QoS in MANETs.

KEY WORDS: Mobile Ad Hoc Networks, Trust Management, Security Enhancement and QoS

I. INTRODUCTION

A recent advances in wireless technologies and mobile devices, Mobile Ad hoc Networks (MANETs) have become popular as a key communication technology in army tactical environments such as establishment of communication networks used to coordinate army deployment among the soldiers, vehicles, and operational command centers. There are many risks in army environments needed to be considered seriously due to the distinctive features of MANETs, including open wireless transmission medium, nomadic and distributed nature, lack of centralized infrastructure of security protection . Therefore, security in tactical MANETs is a challenging research topic. There are two complementary classes of approaches that can safeguard tactical MANETs: prevention-based and detection based approaches Prevention-based approaches are studied comprehensively in MANETs. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed, which may not be realistic in distributed networks such as MANETs. In addition, a centralized infrastructure will be the main target of rivals in battlefields. If the infrastructure is destroyed, then the whole network may be paralyzed . Furthermore, although prevention-based approaches can prevent misbehavior, there are still chances remained for malicious nodes to participate in the routing procedure and disturb proper routing establishment. From the experience in the design of security in wired networks, multi-level security mechanisms are needed. In MANETs, this is especially true given the low physical security of mobile devices. Serving as the second wall of protection, detection-based approaches can effectively help identify malicious activities. Although some excellent work has been done on detection based approaches based on trust in MANETs, most of existing approaches do not exploit direct and indirect observation (also called secondhand information that is obtained from third party nodes) at the same time to evaluate the trust of an observed node. Moreover, indirect observation in most approaches is only used to assess the reliability of nodes, which are not in the range of the observer node. Therefore, inaccurate trust values may be derived. In addition, most methods of trust evaluation from direct observation do not differentiate data packets and control packets. However, in MANETs, control packets usually are more important than data packets.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

II. RELATED WORK

In the related work, the terms trust and trustworthiness seem to be interchangeably used without clear distinction. Josang et al. clarified the difference between trust and trustworthiness based on their definitions provided by Gambetta . The level of trust is defined as the belief probability varying from 0 (complete distrust) to 1 (complete trust) In this sense, trustworthiness is a measure of the actual probability that the trustees will behave as expected. Solhaug et al. define trustworthiness as the objective probability that the trustee performs a particular action on which the interests of the trustor depend. An explains how trust (i.e., subjective probability of trust level) and trustworthiness (i.e., objective probability of trust level) can differ and how the difference affects the level of risk the trustor needs to take. In the diagonal dashed line is assumed to be marks of well-founded trust in which the subjective probability of trust (i.e., trust) is equivalent to the objective probability (i.e., trustworthiness). Depending on the extent to which the trustor is ignorant about the difference between the believed (i.e., trust) and the actual (i.e., trustworthiness) probability, there is inconclusiveness about or a miscalculation of the involved risk. That is, the subjective aspect of trust brings incorrect risk estimation and wrong risk management accordingly.. Even though risk is an intrinsic characteristic of trust, even well-founded trust, misplaced trust increases risk and thus the chance of deceit,

III. TRUST MANAGEMENT MODEL

We discuss a trust management model based on the concept of social and cognitive networks. In addition, we list several issues and developers of MANET trust management model should keep in mind. MANETs pose challenges in designing network security protocols due to their unique characteristics (e.g., resource constraints, vulnerability, unreliable transmission medium, and dynamics). Army MANETs must operate in hostile environments, deal with compromised nodes, support prioritized QoS performance, be able to participate in coalition operations without predefined trust relationships, and facilitate reconfigurability. Thus, additional caution is required in designing security protocols for mission-driven group communication systems in Army MANETs. We are particularly interested in evaluating the trust level of such a group communication systems by evaluating the trust value of a node in terms of its mission execution competence and sociability when a particular mission. That is, our trust management protocol aims to dynamically reconfigure the trust threshold that determines the number of nodes qualified for performing the mission. We take into account the level of risk or difficulty upon failure while considering changing network conditions (i.e., bandwidth, node density, communication rate, degree of hostility) as well as the conditions of participating nodes in the network (i.e., energy, computational power, memory). As a result, the resulting protocols seek to prolong the system lifetime by identifying optimal design settings such as trust value threshold to determine trustable nodes to perform a mission, degree of trust transitivity chains, ratio of trust attributes (i.e., ratio of social trust versus QoS trust, We explained in conditional tolerance threshold of selfish behaviors, and length of trust chains based on efficient tradeoffs made between security and performance properties. Unlike existing work on trust management in MANETs, our research proposes to embed intelligence in each node with cognitive functionality, adopting recent ideas about cognitive networks in wireless networks. Current network conditions and then planning, deciding, and acting on those conditions. Cognitive networks are able to reconfigure the network infrastructure based on past experiences by adapting to continuously changing network behaviors to improve scalability (e.g., reducing complexity), survivability (e.g., increasing reliability), and QoS level (e.g., facilitating cooperation among nodes) as a forward looking mechanism . Cognitive networks are also often based on cross-layer design where they share internal information between layers rather than adhering to the traditional strict layered architecture define a social network as a social structure of individuals who may be related directly or indirectly to each other in order to pursue common interests. Yu et al. used social networks to evaluate the overall trust value of a node. However, we use social networks to evaluate the social trust value of a node only in terms of the degree of personal or social trends, rather than the capability of executing a mission based on past collaborative interactions. We assume that a node's capability of completing a highly risky mission will be related to the node's QoS trust value as evaluated by information networks based on information sharing.

IV. EXISTING SYSTEM

In the existing system there are two complementary classes of approaches as prevention based approaches and detection based approaches. In the first approaches, a centralized key management infrastructure will be maintained. But the centralized infrastructure will not be realistic to the in distributed network such as MANET, more over when

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

that infrastructure will be destroyed the whole network will be damaged. In the second method, it effectively prevents the malicious activities. Even though it prevents still there is a malicious attack and packet loss in the network

V. PROPOSED SYSTEM

In this paper, we develop a trust management scheme which uses a uncertainty reasoning to evaluate trust value of each and every node. The trust value is a degree of belief that a node performs as expected. The difference between our proposed scheme and the existing one is that we are identifying the trustworthy node and then derive our path to send packets. Our proposed system includes the following outlines. The trust scheme in this paper includes two types of observations.1.Direct observation 2.Indirect observation. A direct observation we use the Bayesian inference which is a type of uncertainty reasoning to calculate the trust value. The source node will directly observes its destination An indirect observation we use the dempster-shafer theory. The trust value will be calculated from the neighbor node of the observer node. Finally we evaluate our proposed scheme in the routing procedure of the MANET to send the packet more secure and successful.

VI. COMPONENTS OF SECURITY ENHANCEMENTS OF MANET

Based on the definition, we depict the trust model that is used to formulate the trust between two nodes in MANETs, and present a framework of the proposed scheme. Trust has different meanings in different disciplines from psychology to economy. The definition of trust in MANETs is similar to the explanation in sociology, where trust is interpreted as degrees of the belief that a node in a network (or an agent in a distributed system) will carry out tasks. Due to the specific characteristics of MANETs, trust in MANETs has five basic properties: subjectivity, dynamicity,non-transitivity, asymmetry, and context-dependency. Subjectivity means that an observer node has a right to determine the trust of an observed node. Different observer nodes may have different trust values of the same observed node. Dynamicity means that the trust of a node should be changed depending on its behaviors. Non-transitivity means that if node A trusts node B and node B trusts node C, then node A does not necessarily trust node C. Asymmetry means that if node A trusts node B, then node B does not necessarily trust node A. Context-dependency means that trust assessment commonly bases on the behaviors of a node. Different aspects of actions can be evaluated by different trust. For example, if a node has less power, then it may not be able to forward messages to its neighbors. In this situation, the trust of power in this node will decline, but the trust of security in this node will not be changed due to its state.

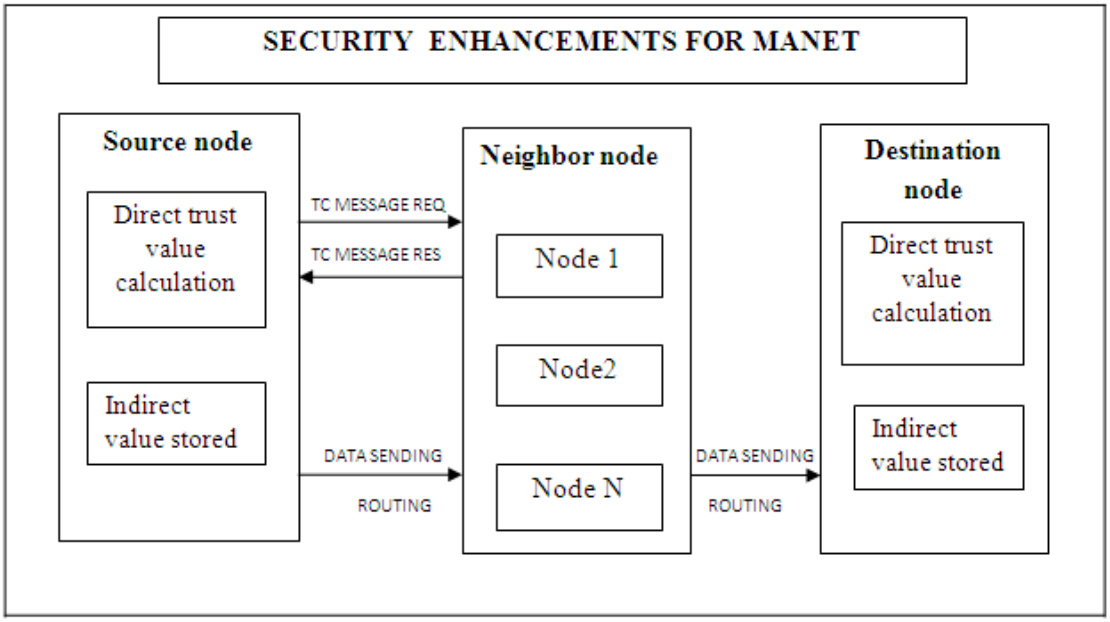

Figure1. Architecture diagram for Security Enhancement for MANET

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

In the direct observation method the observer will directly observes its neighbor node. The observer node will overhear its neighbor whether it receives the packet correctly. Therefore the node will calculate the trust value of its neighbor using Bayesian inferences. Whenever the neighbor sends the packets correctly the forwarded packet value will be increments in observer side. In case of packet loss it will be decrements and also the punishment factor will be maintained for each neighbor nodes. Past experience is also an important factor when trust values are calculated. Recent activities of the node are seriously affecting the trust evaluation. The punishment factor is used to give more weights on misbehavior in the Bayesian framework. Firstly, this can lower the trust of an attacker when it misbehaves. Secondly ,the trust value of a attack will not be recover quickly even if it forwards large number of packets correctly due to the impact of punishment factor. By this values trust value will be calculated $T^{S.}$ An indirect observation method the trust value will be calculated from the testimonies of the neighbor nodes. The neighbor nodes will send the trustworthiness of the observed node to the observer node. This may reduce the bias from observer. The opinions will be asked from collection of neighbors so that the node act malicious to one node and good to other will be easily found out and eliminated. Every node needs to records its one-hop neighbors, how many data packets each neighbor received and how many data packets each send correctly. TC messages only recorded for trust value calculation. When a node receives a packet the number of packet receives will be increased. if the node forwards the packet correctly the number of packet forwards will be increased by one. Dempster-Shafer theory is used by indirect method .The trust value is calculated as T^N. After T^N and T^S are obtained we get the whole trust value. we are obtainable to derive the shortest path considering both trust value and hop counts and use the Dijstra's algorithm to calculate the best routing path. Since minimization is used in Dijstra's algorithm so we have to convert the trust value to untrustworthy value. Using this process we can find a short and a secure path.

VII. CONCLUSION

The objective of this paper was to provide MANET network protocol designers with multiple perspectives on the concept of trust management model. By introducing the concept of social and cognitive networks, we suggested future research directions to develop trust management model with desirable attributes such as adaptation to environmental dynamics, scalability, reliability, and reconfigurability. Trust is a multidimensional, complex, and context-dependent concept. Although, trust-based decision making is in our everyday life, trust establishment and management in MANETs faces challenges from the severe resource constraints, the open nature of the wireless medium, the complex dependence between the communications network, the social network, and the application network, and hence the complex dependency of any trust metric to features, parameters, and interactions within and amongst these networks.

REFERENCES

[1]. Corson and J. Macker, "Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations," IETF RFC 2501, Jan. 1999.
[2] F. R. Yu, Cognitive Radio Mobile Ad Hoc Networks. New York: Springer, 2011.
[3] J. Loo, J. Lloret, and J. H. Ortiz, Mobile Ad Hoc Networks: Current Status and Future Trends. CRC Press, 2011.
[4] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks," EURASIP J.Wireless Commun. Networking, vol. 2013, pp. 188–190, July 2013.
[5] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," IEEE Trans. Wireless Commun., vol. 13, pp. 1616–1627, March 2014.
[6] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," IEEE Trans. Dependable and Secure Computing, vol. 3, pp. 386–399, Oct.–Dec. 2006.
[7] Y. Fang, X. Zhu, and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," IEEE Wireless Comm., vol. 16, no. 2, pp. 24–30, 2009.
[8] F. R. Yu, H. Tang, P. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," IEEE Trans. on Network and Service Management, vol. 7, pp. 258 –267, Dec. 2010.
[9] P. Albers, O. Camp, J.-M. Percher, B. Jouga, and L. M. R. S. Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches," in Proc. 1st Int'l Workshop on Wireless information Systems, (Ciudad Real, Spain), Apr. 2002.
[10]. Eschenauer, V. D. Gligor, and J. Baras, "On Trust Establishment in Mobile Ad Hoc Networks," Proc. 10th Int'l Security Protocols Workshop, Cambridge, U.K., Apr.2002, vol. 2845, pp. 47-66.