SECURE ON-DEMAND ROUTING PROTOCOL USING FRIENDSHIP MECHANISM

[1]R.VIJAYAKUMAR [2]PL.THENUPRIYA [3]R.SRUTHI [4]V.RAMYANIVEDITHA
Research Scholar **Final Year – Computer Science and Engineering,**
msgvijaykumar@gmail.com thenupriya92@gmail.com sruthirp13@gmail.com ramyaniveditha222@gmail.com
Sri Ramakrishna Engineering College,
Coimbatore.

Abstract A Mobile Ad-hoc Network (MANET) is a collection of wireless nodes that can be dynamically set anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile host connected by of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. MANET can operate without fixed infrastructure and can survive rapid changes in the network topology. In this paper we have presented a trust based on-demand routing protocol using friendship mechanism. This mechanism is used to find the secure path to transfer data between nodes and evaluate their performance with respect to performance metrics like packet delivery ratio, End-to-End delay, Friendship Message activity. The main method for evaluating the performance of MANETs is simulation and we prefer Network Simulator (NS2).

Keywords Manet, Source Routing, Malicious node, Trust Prediction

IJSER

INTRODUCTION:

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage communication between moving body and moving body and fixed objects. Mobile Computing is when a (work) process is moved from a normal fixed position to a more dynamic position. A Mobile Ad-hoc Network is a collection of wireless nodes that can dynamically be set up anywhere and
anytime without using any pre-existing network 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; Therefore, the limited wireless transmission range of each node gets extended by multihop packet forwarding. This kind of network is well suited for the mission critical applications such as emergency relief, military operations, and terrorism response where no pre deployed infrastructure exits for communication. Due to its intrinsic nature of lacking of any centralized access control, secure boundaries(mobile nodes are free to join and leave and move inside the network) and limited resources mobile Ad-hoc Networks are vulnerable

to several different types of attacks such as redirection attack ,worm hole, black hole and so on.

Many researchers have been proposed to secure the routing protocols. In this research we focus on securing the securing the AODV routing protocols. SAODV protocol has been proposed to secure AODV in which both AODV messages (RREQ, REP) and the mutable information (hop count, hash value) is included in the protection mechanism. Each node signs RREQ and RREP message after reducing the hop count and the hash value fields, in which these fields are changed in every hop. The signing process is accomplished by using asymmetric cryptography. SAODV can defend against black hole attack. However, it cannot defend against worm-hole attack, hop-count altering attack and routing messages dropping attack.

In this paper, friendship based AODV routing protocol has been implemented in a simulation mode (using NS2). Some trust features are identified to evaluate the node friendship in the network. A friendship mechanism algorithm is constructed to secure AODV routing protocol. This paper is organized as follows: Section 2 describes some related works about MANET and trust prediction. Section 3 presents our proposed friendship mechanism for on-demand routing protocol scheme. The performance evaluation of our proposed scheme for simulation is presented in Section 4. The paper is concluded with suggestion for future work.

2. Related works

2.1 Defense in MANET

The specific features of MANETs present a challenge for security solutions. Many existing security solutions for conventional networks are ineffective and inefficient for many envisaged MANET deployment environments. Consequently, researchers have been working for the last decade on developing new security solutions or changing current ones to be applicable to MANETs. Since many routing protocols do not consider security, some research focuses on developing secure routing protocols or introducing security extensions to the existing routing protocols. Routing protocols have been proposed to counter selfish activities by forcing the selfish nodes to cooperate. Existing key management mechanisms are usually based on central points where services such as certification authorities or key servers can be placed. Since MANETs do not have such points, new key management mechanisms have had to be developed to fulfill requirements. Finally, since prevention techniques are invariably limited in effectiveness, intrusion detection systems are generally used to complement other security mechanisms. This applies to MANETs too and researchers have proposed new mechanism to detect malicious activities on these networks.

H Yang H Y. Luo[2] focus on the fundamental security problem of protecting the multihop network connectivity between mobile nodes in a MANET. They identify the security issues related to this problem, discuss the challenges to security design, and review the state-of-the-art security proposals that protect the MANET link- and network-layer operations of delivering packets over the multihop wireless channel. The complete security solution should span both layers, and encompass all three security components of prevention, detection, and reaction.
MANETs have unique characteristics and constraints that make traditional approaches to security inadequate. In particular, it is not appropriate to assume preexisting shared secret keys or authentication among members. The lack of an infrastructure exacerbates the situation. Therefore the issues of authentication, key distribution, and intrusion detection require different methods, which are discussed here. Traditional authentication, key distribution, and intrusion detection methods are often too inefficient to be used in resource-constrained devices in MANETs. G.V.S Raju[3]propose to combine efficient techniques from elliptic curve cryptography (ECC) and a distributed intrusion-detection system (IDS) based on threshold cryptography and also propose to use a distributed certifying authority (CA) along with per packet and per-hop authentication for addressing the issues mentioned above. The model assumes that no single node can be trusted and relies instead on a distributed trust model. In these mainly focused on cryptography to transfer data between source and destination and they also mentioned distributed concept here.

2.2Conviction prophecy of MANET

Tameem Eissa and Shukor Abdul Razak [4] proposed the challenging issues in routing security and also presents a trust-based scheme for securing AODV routing protocol in MANET using the friendship mechanism. Here nodes can evaluate the routing paths according to some selected features (such as node reputation and identity information) before forwarding the data through these routes. Many researchers have proposed different methods to secure the routing protocols. In this research, we focus on securing AODV routing protocol. SAODV protocol has been proposed to secure AODV [5], in which both AODV messages (RREQ, RREP) and the mutable information (hop count, hash value) is included in the protection mechanism. Each node signs RREQ and RREP message after reducing the hop count and the hash value fields, in which these fields are changed in every hop. The signing process is accomplished by using asymmetric cryptography.

Kannan Govindan and Prasant Mohapatra [6] presented a detailed survey on various trust computing approaches that are geared towards MANETs. Trust is an important aspect of mobile adhoc networks (MANETs). It enables entities to cope with uncertainty and uncontrollability caused by the free will of others. Trust computations and management are highly challenging issues in MANETs due to computational complexity constraints, and the independent movement of component nodes. This prevents the direct application of techniques suited for other networks. In MANETs, an untrustworthy node can wreak considerable damage and adversely affect the quality and reliability of data. Therefore, analyzing the trust level of a node has a positive influence on the confidence with which an entity conducts transactions with that node. Trust computations are challenging because:

- There could be different types of mobility in MANETs such as low mobility (human walking with sensors) or high mobility (mobility of sensors mounted on vehicle). The network composition may significantly change with time in an unpredictable manner due to this mobility. When

the neighbor constantly changes, it becomes difficult to make observation and get enough opportunities for interactions to measure the trust. Information received from the MANET nodes are more valuable and trustworthy if they can be related to where and when the readings originated [9]. However, when the location is constantly changing, it is hard to associate the information and node behaviour with locations.

• In the absence of centralized control station, monitoring the behaviour of nodes is very difficult. The complexity in trust computations grows non-linearly without the centralized command center. The worst case complexity of obtaining the trust level on every node by every other node in a network of N connected nodes is O(N2). Another work included here is trust system contains the following functional blocks: trust computation based on metrics, trust propagation, trust aggregation, trust prediction and trust applications.

In the human society, trust is one of the most common concepts, while trust depends on a host of factors which can't be easily modeled by the computational methods. In the areas of computer science, trust has been used in many fields to mean many different things. For example, it's a descriptor of security and encryption; a name for authentication methods or digital signatures; a measure of the quality of a peer in P2P systems; a factor in game theory; a model for agent interactions; a gauge of attack resistance; a component of ubiquitous and distributed computing; a foundation for interactions in agent systems; or a motivation for online interaction and recommenders systems [8].

3. Our Proposal

In this scheme we have presented the friendship based frame work to secure AODV routing protocols. Each node has identity information which cannot be attacked by malicious nodes. The identity information smart card for simplicity we use MAC and IP addresses. And we also assume that number of malicious nodes is less than the good nodes.

3.1 Friendship based secure routing protocols

In this scheme i.e in friendship based mechanism each node will have a list of friends and their values those values are in the range from 0 to 100. Trust on these nodes depends upon their value, bigger their value is more they are trusted. Two algorithms are used to create the trust routes which are Rvevaluate and Fwevaluate algorithm. The estimation of the node depend on their value, higher the value is the more trustworthiness is granted to the node. If the friendship value is less than TF(Threshold Friendship) it is said to be malicious. TF value can be assigned by the designer according to the scenario, if the TF value is lesser than the assigned value the communication from the specific node is blocked.

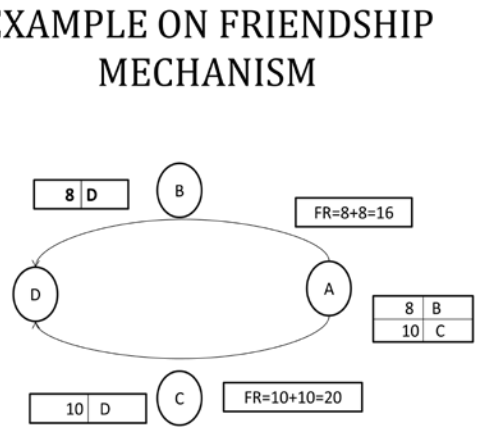

Fig 1 Example on Friendship Mechanism

Figure 1 shows the example for friendship mechanism. Node A is the source node and node D is the destination. In this example the source node transfers the data to the destination through node B or C. Let us assume value for nodes, for transferring the data through the nodes A-B-D the friendship value is 16 (A-8, B-8), the route A-C-D the friendship value is 20 (A-10 C-10). The friendship value for the route A-C-D is higher when compare to the other node, so the this route is chosen for data transfer.

3.2 Node Authentication in secure routing protocols

The IP and MAC addresses are used as the identity for the authentication purpose. There are two authentication which are Logical address authentication and physical address authentication. The Logical authentication is that in which a node associates with a new node based on the MAC address. In the Physical authentication the source node can directly communicate with new nodes.

Routing packets carry the sequence numbers. The maintenance of timer-based states in each node for utilization of individual route entries is an important feature of AODV protocol. Based on the packet delivery ratio the DSR performance is better than the AODV protocol.

4. Conclusion

In this paper we have shown that the friendship mechanism is used to secure routing protocol in MANET. We also have evaluated the nodes using the trust concepts.
In future we have planned to implement the friendship mechanism in all other routing protocols and the comparison of the protocols using various performance metrics.

References

1. A secure routing protocol for ad hoc networks. Sanzgiri K, Dahill B, Levine BN, Shields C, Belding-Royer EM In Proceedings of the 10th IEEE International Conference on Network Protocols, ICNP '02, pp 78–89, Washington, DC, USA, 2002. IEEE Computer Society

2. Security in mobile ad hoc networks: Challenges and solutions. H Yang H Y, Luo F Ye S W,Lu L Zhang University of California Postprints Year 2004, Paper 618

3. Mobile Ad Hoc Networks Security.G.V.S. Raju ,Rehan Akbani University of Texas at San Antonio. Annual review of communication, volume 58.

4. Trust-Based Routng Mechanism in MANET Design and Implementation. Tameem Eissa, Shukor Abdul Razak, Rashid Hafeez Khokhar, Normalia Samian Mobile Netw Appl Springer Science Business Media, LLC 2011.

5. Securing ad hoc routing protocols.Zapata MG, Asokan N (2002) In Proceedings of the 1st ACM workshop on Wireless security, WiSE '02, pp 1–10, New York, NY, USA. ACM.

6. Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey.Kannan Govindan, Prasant Mohapatra, University of California Davis, CA- 95616.

7. Trust Evaluation and Dynamic Routing Decision Based on Fuzzy Theory for MANETs.Hongjun Dai, Zhiping Jia and Zhiwei Qin, JOURNAL OF SOFTWARE, VOL. 4, NO. 10, December 2009.

8. Trust and for Reputation service oriented environment Change. E, Dillon T, and Hussain. F, John Wiley and Sons, 2005.

9. Ad-hoc on-demand distance vector routing.Perkins CE, Royer EM (1999) In Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, pp 90–100, Feb 1999

10. Highly reliable trust establishment scheme in ad- hoc networks.Ren K, Li T, Wan Z, Bao F, Deng RH, Kim K (2004) Comput Netw 45:687–699.

11. An effective trust establishment scheme for authentication in mobile ad hoc net- works. Wang G, Wang Q, Cao J, Guo M (2007), pp 749–754, Oct

12. Architectural support for trust models in decentralized applications. G. Suryanarayana, M. H. Diallo, J. R. Erenkrantz, and R. N. Taylor, in Proc. 28th Int. Conf. Softw. Eng., May 2006, pp. 52-61.

13. Reputation based framework for high integrity sensor networks S. Ganeriwal and M. B. Srivastava, ,in Proc. ACM Security for Ad-Hoc and Sensor Netw., 2004, pp. 66-67.

14. A trust-based security system for ubiquitous and pervasive computing environments, A. Boukerche and Y. Ren, Computer Communications, vol. 31, pp. 4343-4351, 2008.

15. Trust establishment in pure ad hoc networks, A.Pirzada and C. McDonald, Wirel. Pers. Commun., vol. 37, no. 1/2, pp. 139-168, Apr. 2006.

IJSER