Secured Multi Path Routing with Trust Establishment Using Mobile Ad Hoc Networks

T. Nirmal Raj, S. Saranya, S. Arul Murugan, G. Bhuvaneswari

Abstract - We propose a novel method of message security using trust-based multi-path routing. Simulation results, coupled with theoretical justification, affirm that the proposed solution is much more secured than the traditional multi-path routing algorithms. We propose a method to securely route messages in an ad-hoc network using multi-path routing and trustworthiness of the nodes. Hence, we aim at addressing the issues underlying message confidentiality, message integrity and access control. We combine multi-path routing and trust with soft encryption technology to propose a scheme which is much more secure than traditional multi-path algorithms. By soft encryption, we mean having encryption methods, but are more efficient in terms of performance and require less resource.

Keywords: Trust, Misbehaving nodes, soft encryption, Dynamic Source Routing, Multi-path routing.

1. INTRODUCTION

A mobile ad hoc network (MANET) is a kind of wireless ad hoc network, and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Mobile ad hoc networks (MANETs) are composed of a set of stations (nodes) communicating through wireless channels, without any fixed backbone support. With the advancement in radio technologies like Bluetooth, IEEE 802.11 or hiperlan, a new concept of networking has emerged which makes wireless networks increasingly popular in the computer industry. This is particularly true within the past decade, which has seen wireless networking being adapted to enable mobility.

Later on numbers of different protocol have been proposed as a routing solution for mobile ad hoc networks. These different routing techniques classified as proactive, reactive and hybrid routing protocols. Reactive routing protocols have been found to be user friendly and efficient when compared to other routing protocols. The main boon of Reactive routing protocols when compared with Proactive and Hybrid routing protocols is the relatively unconditional low storage requirements, higher mobility and the availability of routes when needed. There are a variety of reactive routing protocols such as AODV, DSR, LAR1, LMR, ABR, SSI, TORA, RDMAR, MSR, AOMDV, MRAODV, ARA. Most of the multipath routing protocols like AOMDV, MP-OLSR and MP-DSR are the extension of unipath protocols like AODV, OLSR and DSR. In these protocols we use the DSR in this paper. DSR is the next generation pure reactive routing protocol for MANETs. It was proposed for the first time by Johnson and Maltz [5] in order to provide routing with minimum overhead while adapting to the network dynamics.

DSR is undergoing fast evolution thanks to the many optimizations integrated into it. DSR is based on a pure reactive approach and operates using two simple and complementary mechanisms: route discovery and route maintenance. In this paper We propose a novel method of message security using trust-based multi-path routing we propose a method to securely route messages in an ad-hoc network using multi-path routing and trustworthiness of the nodes. We aim at addressing the issues underlying message confidentiality, message integrity and access control.

2. RELATED WORKS

Security in MANETs has been a topic of much discussion in the last few years. There are a plenty of works available in the literature that discuss security in MANETs. But efficiently providing complete message security in such networks still remains an open issue.

Much research work has been done to make the route discovered by Dynamic Source Routing (DSR) secure. A Trust based multi path DSR protocol is proposed by Poonam et al. [11] in which uses multi-path forwarding approach. In this approach each node forwards the RREQ if it is received from different path. Through this method detect and avoid misbehaving nodes which were previously included due to vulnerability in DSR route discovery. In the traditional DSR protocol [5] when a node receives a RREQ packet, it checks if it has previously processed it, if so it drops the packet. A misbehaving node takes advantage of this vulnerability and forwards the RREQ fast so that the RREQ from other nodes are dropped and the path discovered includes itself. In their protocol

each node broadcast the packet embedding trust information about the node from which the packet is receive. At the source node a secure and efficient route to the destination is calculated as weighted average of the number of nodes in the route and their trust values.

All the existing models have one or more of the following limitations. Most of the methods use the traditional DSR request discovery model, in which a node drops a RREQ packet, if it has previously processed it. A misbehaving node takes advantage of this and forwards the RREQ packet fast so that the RREQ received from other nodes, which arrive later, are dropped and the path discovered includes itself. Most of the trust based routing protocols have used forward trust model to find the path from source to destination. In this model trust is embedded only in the RREQ packet when it is forwarded. So each node evaluates only its previous node and the source node evaluates all the nodes involved in path. But we believe that the trust is asymmetric, so mutual trust information should be used. In watch dog and pathrater approach the trust values are not updated based on node behavior, rather they are updated periodically. Such periodic updates are not able to quantify the misbehaving nodes. Therefore the path discovered includes misbehaving nodes. All of these possible vulnerabilities have been taken care of in [11]. The authors have designed a secure routing protocol, called Trust based multi path DSR protocol, which depends on two-way effort of the node by embedding trust to find an end-toend secure route free of misbehaving nodes. This protocol has a drawback routing overhead is very high compared to traditional DSR due to broadcasting of RREQ packet. The other drawback is that all the one hop neighbors of destination after receiving first RREQ propagate to destination and also among them. Then this results in discarding the RREQ packet from most of the other paths to the destination node.

3. GLOMOSIM

Glomosim is a library-based sequential and parallel simulator for wireless networks. This has been developed using PARSEC, a C-based parallel simulation language. Glomosim can be modified to add new protocols and applications to the library. Therefore Glomosim is a good choice for implementing the different traffic sources.

4. TRUST BASED MULTI-PATH ROUTING WITH SOFT ENCRYPTION TECHNOLOGY

We propose a method to securely route messages in an ad-hoc network using multi path routing and trustworthiness of the nodes. Hence, we aim at addressing the issues underlying message confidentiality, message integrity and access control. We divide the message into different parts and encrypt these parts using one another. We then route these parts separately using different paths between a pair of source-destination nodes. An intermediate node can access different parts on the basis of its trustworthiness. That is, a more trusted node is allowed to feature in more paths than a less trusted node and hence access to more message parts than a less trusted node. This feature allows the routing algorithm to avoid nodes that are more likely to attempt 'breaking-in' the encryption. In addition, suspected nodes which have high computation power and are hence likely to be more successful in cryptanalysis can be given less parts to stymie their plans. Since establishment of trust also requires cryptographic key exchange, we use a soft approach to trust. Trust levels of peer nodes of the network are found using effort return based trust model. We use a variation of the model, which uses a combination of derived trust and reputation to estimate trust values of a node.

We combine multi-path routing and trust with soft encryption technology to propose a scheme which is much more secure than traditional multi-path algorithms. Networks using the DSR protocol have been connected to the internet. DSR can interoperate with mobile IP, and nodes using mobile IP and DSR have seamlessly migrated between WLANs, cellular data services, and DSR mobile ad hoc etworks. The DSR protocol include easily guaranteed loop-free routing, support for use in networks containing unidirectional links, use of only "soft state" in routing, and very rapid recovery when routes in the network change. This is the reason for preparing to the DSR protocol.

4.1 SOFT ENCRYPTION TECHNIQUES AND ROUTING

A 4n-bits message is divided into four parts of n bits each. Let us denote these parts by a, b, c and d. We define the bit operation XOR on bit vectors k and l as follows:

If k = {k1, k2, k3…, kn}
And l = {l1, l2, l3, …, ln}
Then
$k \text{ XOR } l = \{k_1 \text{ XOR } l_1, k_2 \text{ XOR } l_2, k_3 \text{ XOR } l_3, \ldots; k_n \text{ XOR } l_n\}$

The aforementioned parts a, b, c, and d are then encrypted by means of the following equations:

a′ = a XOR c

b′ = b XOR d

c′ = c XOR b

d′ = d XOR a XOR b

The parts a′, b′, c′ and d′ are now routed instead of a, b, c and d. Paths between the source and destination nodes are found using DSR. A node waits for intermediate multiple paths to the destination. Routing paths are selected from

The set of paths using a novel trust defined strategy.

At the destination node, the message parts can be decrypted using the following equations:
a=b′ XOR d′
b=a′ XOR b′ XOR c′ XOR d′
c=a′ XOR b′ XOR d′
d=a′ XOR c′ XOR d′

4.2 TRUST ESTABLISHMENT

A node is assigned a discreet trust level in the range of -1 to 4. A trust level of 4 defines a complete trust and a trust level of -1 defines a complete distrust. These trust levels also define the maximum number of packets, which can be routed via those nodes. A trust level of -1 signifies that any packet coming from that node should be dropped. No packet is in turn routed to these nodes, leading to an isolation of malicious nodes.

4.3 TRUST LEVELS ASSIGNMENT

The trust level assigned to a node is a combination of direct interaction with its neighbours and the recommendations from its peers. A node assigns a direct trust level to its neighbour on the basis of the acknowledgements received. If the neighbour sends a prompt acknowledgement of the packet received, it is assumed that the node is not involved in a resource intensive brute-force attack and hence is assigned a higher trust level. The direct trust is then combined with the trust recommendation from its peers and a final trust level is assigned to it. But these trust levels are assigned dynamically and are cached by a node for performance enhancement. The trust recommendations are piggybacked on DSR routing packets.

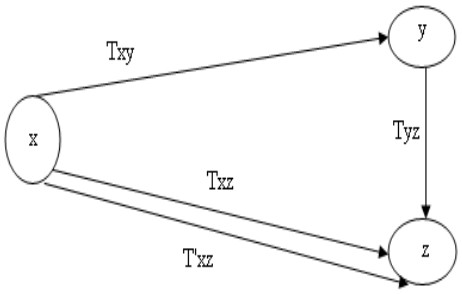


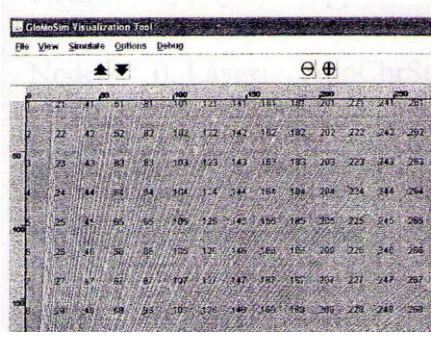
Figure 1: **Trust levels assignment**

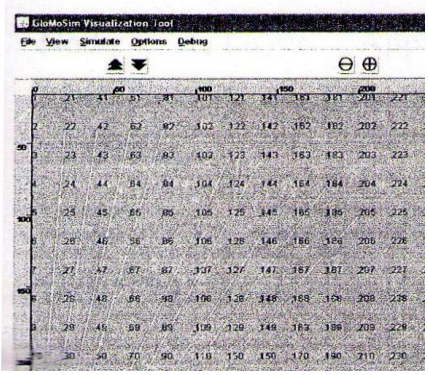
Let us consider that T_{xy} represents the direct trust in node Y by node X, and let T_{yz} represents the trust recommended by the node Y in node Z. If T'_{xz} represents the direct trust of node Z in node X, then the trust assigned by X in Z.
$T'_{xz} = 1- (1- T_{xz}).(1- T_{xyz})$

Where $T_{xyz} = 1 -(1- T_{xy}) T_{yz}$

The trust levels are normalized to integer values using standard methods. Each node is given an integer trust value lying between -1 and 4. If a new node joins the network, it sends a hello packet to its neighbours. The neighbours would assign an initial trust value of 0 to the node. The trustworthiness of the node can be increased if the node shows benevolent behaviour. Similarly, when a node leaves the network, it would no longer respond to the messages. The neighbour may conclude that the network has lost its connectivity or the node has exited the network.

5. RESULT





6. CONCLUSION

The simulation experiments conducted were evaluated in Global Mobile Information System Simulator (GloMoSim). GloMoSim is a scalable simulation environment for large wireless and wire line communication systems using parallel discreet-event simulation language called PARSEC. GloMoSim is an event based system coded in C. GloMoSim implements all the seven layers of the ISO-OSI reference model and is customizable and assessable at all the layers. It supports various pre compiled models and protocols at various layers including the DSR routing algorithm at the network layer, which was used as a basis for our system. On the Medium Access Control(MAC)layer, protocols such as CSMA, FAMA,MACA and IEEE 802.11 are currently available. On the application layer, models such as TCPLIB, CBR (Constant Bit Rate) and HTTP traffic are supported. It is at the application layer that the soft encryption using various message parts is implemented.

We discussed various methods that have been proposed and highlighted their respective advantages and limitations in various scenarios. We have provided some ideas of possible solutions to these problems and we have discussed how our proposed system can incorporate these solutions. Based on these settings, we have introduced a trust based multi-path algorithm for message security in MANETs. We have discussed the message encryption and the trust establishment methodologies that can be used in the system. Then, we have proposed a trust based strategy for route selection. The implementation of this trust-based approach using DSR was then discussed. Finally, the simulation results obtained from our algorithm are compared against the results obtained using traditional algorithms such as normal DSR and multi-path routing using disjoint paths, used as benchmarks. Our proposed solution proved to be much more secured than the results obtained from traditional multi-path routing algorithms.

7. REFERENCES

[1] Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y.C. and Jetcheva, J. G. 1998 A performance comparison of multihop wireless ad hoc network routing protocols. In proceeding of International Conference Mobile Computing and Networking (MobiCom), ACM Press, 85–97.

[2] Buchegger, S. and Boudec, J. 2007. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes—Fairness In Distributed Ad hoc NeTworks. In Proceeding ACM Workshop Mobile Ad Hoc Networking and Computing (Switzerland, 2006). 226-236.

[3] Garfinkel, S.1995 PGP: Pretty Good Privacy. O'Reilly and Associates.

[4] Haniotakis, T., Tragoudas, S. and Kalapodas, C. 2009. Security enhancement through multiple path transmission in ad hoc networks. IEEE Communications Society, 4187-4191.

[5] Johnson, D. B., Maltz, D. A., Hu, Y. C. and Jetcheva, J.G. 2008. The dynamic source routing protocol for mobile ad hoc networks (DSR). Internet draft IETF RFC 3561, http://www.ietf.org/rfc/rfc3561.txt.

[6] Marti, S., Giuli, T. J., Lai, K. and Baker, M. 2006. Mitigating routing misbehavior in mobile ad hoc networks. In Proceeding of Sixth Annual International Conference Mobile Computing and Networking (MobiCom). ACM Press, New York, NY, 255-265.

[7] Narula, P., Dhurandher, S. K., Misra, S. and Woungang, I. 2007. Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing. Elsevier Journal of Computer Communications, 760-769.

[8] Pirzada, A. A., Datta, A. and McDonald, C. 2004. Propagating trust in ad-hoc networks for reliable routing. In Proceeding of IEEE International Workshop Wireless Ad Hoc Networks (Finland, 2004). 58-62.

[9] Pirzada, A. A., Datta, A. and McDonald, C. 2005. Trustbased routing for ad-hoc wireless networks. In Proceeding of. IEEE International Conference Networks (Singapore, 2004). 326-330.

[10] Pissinou, N., Ghosh, T. and Makki, K. 2005. Collaborative trust-based secure routing in multihop ad hoc networks. Networking (Athens, Greece 2005). Lecture Notes in Computer Science, vol. 3042, 1446-1451.

[11] Poonam, Garg, K., and Misra, M. 2010. Trust based multi path DSR protocol. In Proceedings of Fifth

International Conference on Availability, Reliability and Security, (Poland, February, 2010). 204-209.

[12] QUALNET simulator, Available from: <http://www.scalable-networks.com>.

[13] Wang, C., Yang, X. and Gao, Y. 2005. A Routing Protocol Based on Trust for MANETs. In Proceeding of Sixth Annual International Conference on Grid and Cooperative Computing (Beijing, China). Lecture notes in computer science, vol. 3795, 959-964.

[14] Yong, C., Chuanhe, H. and Wenming, S. 2007. Trusted Dynamic Source Routing Protocol. IEEE International Conference on Wireless Communications, Networking and Mobile Computing (Athens, Greece 2007), 1632-1636.

[15] Zhou, L. and Haas, Z. J. 2009. Securing ad hoc networks IEEE Network Magazine, vol. 13, no. 6, 1-12.

AUTHORS PROFILE

T.Nirmal Raj M.Sc,. Mphil working as an Senior Assistant Professor in the Department of Computer Science and Applications in Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya, Enathur, Kanchipuram, Tamil Nadu. He has published more than 5 Papers in National, International journals and conferences. His research interest lies in the area of Network. mailto: tnirmalrajcse@gmail.com

S.Saranya Mphil, Research Scholar in the Department of Computer Science & Applications in SCSVMV University, Enathur, Kanchipuram. She received the degree in Master of Computer Science from Madras University in 2010. She has presented 2 papers in National conference & participated many National and International Conferences. Her interested area in research is Network. mailto: sarandhana889@gmail.com

S.Arul Murugan Mphil, working as a assistant professor in sri sankara arts & science college..He has presented 2 papers in national conference in the area of data mining and warehousing & participated many National and International Conferences.. His area of interest is networking and data mining mailto: arul_jasmines@yahoo.co.in

G.Bhuvaneswari Mphil, Research Scholar in the Department of Computer Science & Applications in SCSVMV University, Enathur, Kanchipuram. She received the degree in Master of Computer Science from Madras University in 2010. She has presented 1 papers in National conference & participated many National and International Conferences. Her interested area in research is Network. mailto: bhuvanagan@gmail.com