International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Trust based Secure Routing in MANET using EAASR

Deepika Mohanan[1], Sachin Godse[2]

[1, 2]Department of Computer Engineering, Sinhagad Academy of Engineering, University of Pune, Kondhwa, Pune, Maharashtra, India

Abstract: ***Mobile ad hoc networks is a system of wireless mobile nodes that can be freely and dynamically self-organized in arbitrary and temporary network topologies without the need of wired or a centralized administration. Mobile ad hoc networks (MANETs) are vulnerable to security threats due to the inherent characteristics of such networks, such as the open wireless medium and dynamic topology. It is difficult to provide trusted and secure communications in adversarial environments, such as battlefields. The adversaries outside a network may deduce the information about the communicating nodes or traffic flows by passive traffic observation, even if the communications are encrypted. The nodes inside the network cannot be always trusted, since a valid node may be captured by rivals and becomes pernicious. As a result, anonymous communications are important for MANETs in adversarial environments, in which the nodes identifications and routes are replaced by random numbers or pseudonyms for protection purpose. Anonymity is defined as the state of being unknown within a set of subjects. The MANETs in adversarial environments, in this the public and group key can be initially deployed in the mobile nodes. It is assumed that there is no online security available when the network is deployed. A key-encrypted onion is used to record a discovered route. Group signature is used to validate the RREQ packet per hop. AASR experiences more cryptographic packet delay. The AASR can be improved by reducing the packet delay for which a unified trust management scheme is added that will enhance the security***

Keywords: Anonymous Routing, Authenticated Routing, Onion Routing, Mobile Adhoc Network, Trust Management

1. Introduction

Idea: Mobile ad hoc networks consist of mobile wireless devices which autonomously organizes their communication infrastructure. Mobile ad hoc networks (MANETs) are vulnerable to security threats due to the intrinsic characteristics of such networks, such as the open wireless medium and dynamic topology. It is difficult to provide trusted and secure communications in adversarial environments.

This has made me to think towards the security of MANET and finding new improved security methods to reduce the attacks made to the network. For this purpose, by referring state of art and finding out how much work has been done in this area, finally come to my Dissertation Topic.

Motivation: IN MANET'S world, devices such as laptops, PCs, cellular phones, appliances with ad hoc communication capability link together on the fly to create a network. This technology is the key to solving today's most common communication problems such as having a fixed infrastructure, and centralized, organized connectivity, etc. MANET is a self-configuring network of mobile routers and associated hosts connected by wireless links. The routers (mobile devices, nodes) are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. The network appears on-demand, automatically and instantly, and data hops from ad-hoc device to device till it reaches its destination, the network updates and reconfigures itself to keep nodes connected. The network topology changes when a node joins in or moves out. Packet forwarding, routing, and other network operations are carried out the by the individual nodes themselves.With each node acting as a router and dynamically changing topology the availability is not always guaranteed. It is also not guaranteed that the path between two nodes would be free of malicious nodes. The wireless links between nodes are highly susceptible to link attacks (passive eavesdropping, active interfering, etc). Stringent resource constrains in MANETs may also affect the quality of security when excessive computations is required to perform some encryption. These vulnerabilities and characteristic make a case to build a security solution, which provides security services like authentication, confidentiality, integrity, non-repudiation and availability. In order to achieve this goal we need a mechanism that provides security in each layer of the protocol. Protection of MANETs can be divided into these two categories, protection of the routing functionality (secure ad hoc routing) and protection of the data in transmission (secure packet forwarding).In the past decades many methods have been formulated for fixing the security issues.

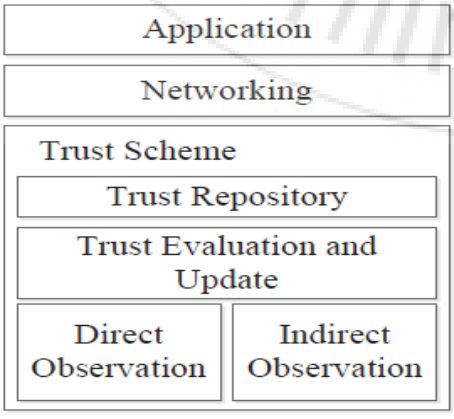
Goal and Objective: Goal of this project is to introduce a new algorithm for reducing the package delay of AASR. The new algorithm used is an unified Trust management model. The objective is to provide anonymity and location privacy, to defend the potential active attacks without unveiling the node identities using group signature, to prevent intermediate nodes from inferring a real destination using onion routing, to improve throughput in the presence of adversary attacks and to reduce the packet loss.

2. Related Work

Anonymous On-Demand Routing (ANODR) Protocol. The first one to provide anonymity and unlinkability for routing in MANET. ANODR uses one-time public/private key pairs to achieve anonymity and unlinkability but fail to guarantee content unobservability. An efficient anonymous routing for MANET, which provides add on advantages for ANODR

protocol is that routing performance changes significantly when different cryptosystems are used to implement the same function. Anonymous Routing (ARM) Protocol uses one-time public/private key pairs and follows only anonymity in route discovery and data forwarding. Discount ANODR achieves substantially lower computation and communication complexities at the cost of a slight reduction of privacy guarantees, but provides only source anonymity and routing privacy. On-Demand Lightweight Anonymous Routing (OLAR) scheme which applies the secret sharing scheme based on the properties of polynomial interpolation mechanism to achieve anonymous message transfer without per-hop encryptions and decryptions. The only task for a forwarder is to perform additions and multiplications, which cost much less than traditional cryptographic operations. Efficient Strong Anonymous Routing (MASR) Protocol which uses onion routing scheme to achieve anonymity but suffers from routing overhead and computation cost. An Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks which adapts onion routing algorithm to achieve anonymity. In this protocol, a node that participates in the protocol encrypts entire message with trust key and says Hello to its ancestor within expiration time. This approach detects the malicious node sand isolate from the network. V-routing based on proactive routing protocol which conceals the location and identity of the communication parties, but it provides weaker security for the data. Anonymous On-Demand Routing (MASK) enables anonymous on-demand routing protocols with high routing efficiency by comparing with ANODR, which is very sensitive to node mobility that may lower routing efficiency. Anonymous routing protocol with multiple routes (ARMR) communications in mobile ad hoc networks and anonymous and secure reporting (ASR) of traffic forwarding activity in mobile ad hoc networks, make use of one-time public/private key pairs to achieve anonymity and unlinkability. ARMR uses one-time public-keys and bloom filter to establish multiple routes for mobile ad hoc networks and ASR is designed to achieve stronger location privacy, which ensures nodes on route have no information on their distance to the source/destination node. Anonymous Location-Aided Routing in Suspicious MANETs uses group signature, but this protocols does not suitable for viable and practical approach to routing in mission-critical location-based environment because no analyses on protocol performance for privacy and security.

3. Methodology



As shown in the above architecture the nodes move through the destination towards the sink. Through the network it is passed across the AASR protocol and the result will be got as the nodes with optimized throughput. There may be some of the errors or problems which can be solved through the trust model.

In the trust scheme component, the module of trust evaluation and update can obtain evidence from direct and indirect observation modules and then utilize two approaches, Bayesian inference and DST, to calculate and update the trust values. Next, the trust values are stored in the module of trust repository. Routing schemes in the networking component can establish secure routing paths between sources and destinations based on the trust repository module. The application component can send data through secure routing paths.

3.1 Network Assumption

3.1.1 Public Key Infrastructure

Let us denote MANET by T. Each node T initially has a pair of public/private keys issued by a public key infrastructure (PKI) or other certificate authority (CA). For node *A* (*A* € T), its public/private keys are denoted by K_{A+} and K_{A-}.

3.1.2 Group Signature

Consider the entire network **T** as a group and each node has a pair of group public/private keys issued by the group manager. The group public key, denoted by G_{T+}, is the same for all the nodes in **T**, while the group private key, denoted by G_{A-} (for *A* € **T**), is different for each node. Node *A* may sign a message with its private key G_{A-}, message can be decrypted as the public key G_{T+} and this and also the anonymity of A is preserved.

3.2 Trust Model

In MANET the definition of trust is very much similar to that of the trust meaning explained in sociology. Therefore trust is explicated as degrees of the belief that a node in a network or an agent in a distributed system will carry out tasks that it should. Due to the specific characteristics of MANETs, trust in MANETs has five basic properties: subjectivity, dynamicity, non-transitivity, asymmetry, and context dependency. trust is made up of two components: direct observation trust and indirect observation trust.

In direction observation trust, an observer evaluates the trust of his one-hop neighbour based on its own opinion. Therefore, the trust value is the assumption of a subjective probability that a trustor uses to decide whether or not a trustee is reliable. The trust value from direct observation and can be calculated by Bayesian inference.

If direct observation is only considered there would be preconception in trust value calculation. To acquire less biased trust value, consider other observers' opinions. With the observer's opinion it can be considered that the method it simply takes arithmetic mean of all trust values which is not adequate to reflect the real meaning of other unreliable observers' opinions as there are two situations that may

severely disturb the effective evidence from neighbors: unreliable neighbors and unreliable observation. Unreliable neighbors themselves are suspects. Even though neighbors are trustworthy, they may also provide unreliable evidence due to observation conditions. Therefore taking all this into consideration the Dempster-Shafer theory is can be thought of as a good candidate to aid in this situation, in which evidence is collected from neighbors that may be unreliable.

Therefore by combining the trust value from direct observation and the trust value from indirect observation, we can get a more realistic and accurate trust value of a node in MANETs.

4. Conclusion

AASR provides higher throughput and lower packets loss ratio in different mobile scenarios in the presence of adversary attacks. It also provides better support for the secure communications that are sensitive to packet loss ratio. AASR can be improved by reducing the packet delay. A possible method is to combine it with a trust based routing. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks. Using recent advances in uncertain reasoning, Bayesian inference and Dempster-Shafer theory, evaluate the trust values of observed nodes in MANETs.

References

[1] J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in *Proc. ACM.*
[2] J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and ondemand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Trans. on Mobile Computing*, vol. 6, no. 8, pp. 888–902, Aug. 2007.
[3] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad hoc Networks," *IEEE Trans. on Wireless Comms.*, vol. 5, no. 9, pp. 2376–2386, Sept. 2006.
[4] J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.
[5] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in *Proc. 2nd Workshop on the Economics of Peer-to-Peer Systems*, (Bologna, Italy), Nov. 2004.
[6] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *Proc. 3rd ACM Workshop on SASN'05*, (Alexandria, VA, USA), Nov. 2005.
[7] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in *Proc. ACM AAMAS'02*, (Bologna, Italy), Jul. 2002.
[8] T. M. Chen and V. Venkataramanan, "Dempster-Shafer theory for intrusion detection in ad hoc networks," *IEEE Internet Comput.*, vol. 9,no. 6, pp. 35–41, 2005.
[9] N. Marchang and R. Datta, "Light-weight trust-based routing protocol for mobile ad-hoc networks," *IET Inf. Secur.*, vol. 6, no. 2, pp. 77–83,2012.

Author Profile

Omkar B. Sawant received the B.E. degree in Computer Engineering from I.C.E.M, Pune, India in 2012 and is pursuing M.E. in Computer Engineering at S.A.O.E, Pune

Sachin P. Godse received the B.E. degree in Computer Engineering from A.V.C.O.E, Sangamner, India in 2004 and M.E. degree in Computer Engineering from S.C.O.E, Pune in 2010. He is currently working as a Professor in S.A.O.E, Pune.