Volume 5, Issue 6, June 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure Routing in MANET using EAASR

Deepika Mohanan, Sachin Godse
Computer Science, Sinhgad Academy of Engineering
Pune, Maharashtra, India

Abstract— Mobile ad hoc networks is a system of wireless mobile nodes that can be freely and energetically self-organized temporary network topologies without the need of a centralized administration. Mobile ad hoc networks (MANETs) are endangered to security threats because of the innate characteristics of such networks. It is very much difficult to provide trusted and secure communications in adversarial environments. The adversaries outside a network may conclude the information about the communicating nodes or traffic flows by passive traffic observation, even if the communications are encrypted. The intermediate nodes that are nodes inside the network cannot be always trusted, since a valid node may be seized by rivals and becomes malicious. Due to this anonymous communications are important for MANETs in adversarial environments, in which the nodes identifications and routes are replaced by random numbers or pseudonyms. 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 are initially established in the mobile nodes. There is no online security available when the network is established. A key-encrypted onion is used so that the discovered route is recorded. Group signature is used to validate the requested packet per hop. AASR experiences more problems of packet delay. AASR can be enhanced by reducing the packet delay for which unified trust management scheme is added to provide security.

Keywords— Anonymous Routing,Authenticated Routing,Onion Routing,Mobile Adhoc Network,Trust Management.

I. Introduction

Due to their natural mobility and scalability, wireless networks are always considered since the day of their development. The improved technology and reduced costs sue to which wireless networks have gained much more importance over wired networks in the past few decades. Rapid development of Mobile Ad Hoc Networks (MANETs) has provoked many wireless applications because of which it can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. Mobile Ad hoc Network (MANET) is a collection of mobile nodes furnished with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. MANETs feature self-organizing and independent infrastructures, due to which it is considered as the absolute choice for uses such as communication and information sharing. Because of the decentralization features of MANETs it is not advisable to compel the membership of the nodes in the network. Nodes in MANETs are endangered to malicious entities that aim to interfere and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols.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 seized by rivals and becomes malicious. As a result anonymous communications are important for MANETs in adversarial environments in which the node identification and routes are replaced by random numbers or pseudonyms for protection purpose. Anonymity in MANETs includes identity and location anonymity of data sources (senders) and destinations (recipients) as well as route anonymity.

Anonymity features ensures that any user may use a resource or service without disclosing the user's identity. Suppose a covert mission is launched, which includes swarms of survey, scrutiny and attacks. In this situation providing anonymity allow the users to interact by hiding their identities from one another and also from third parties. The demand for such anonymity are required in MANET in order to provide user privacy and information security. A number of anonymous routing schemes have been proposed for MANET in which most of them follow on-demand routing approaches. These approaches use various cryptographic operations to anonymize the route discovery and data forwarding processes but not any of the approach provides a complete anonymity with respect to that of unlinkability, unobservability, and pseudonymity.

The first one is unlinkability: to achieve this the routing scheme should provide unlinkability for both content and communicating parties. The unlinkability cites that the content of a message cannot be linked and user unlinkability cites that it cannot be discovered that who communicates with whom. The second is unobservability: to achieve this the routing scheme should provide with unobservability for both messages and traffic pattern. The content unobservability means that important information cannot be extracted from any content and traffic pattern unobservability means that important information cannot be obtained from traffic analyses. The third one is pseudonimity: which provide anonymity to the sender and the receiver. The sender anonymity means that the sender is made anonymous and the receiver anonymity means that the recipient is made anonymous.

Focus is on the MANETs in adversarial environments where the public and group key can be initially deployed in the mobile nodes. It is assumed that there is no online security or localization service available when the network is deployed. Authenticated anonymous secure routing (AASR) is proposed to overcome the pre-mentioned problems. A key-encrypted onion is used to record a discovered route a design an encrypted secret message to verify the RREQ-RREP linkage. Group signature is used to authenticate the RREQ packet per hop to prevent intermediate nodes from modifying the routing packet. Substantial simulations are used to compare the performance of AASR to that of ANODR, a representative on-demand anonymous routing protocol. The results show that, it provides more throughput than ANODR under the packet-dropping attacks although AASR experiences more cryptographic operation delay.

The aim is to introduce a new algorithm for reducing the package delay of AASR. The unified Trust management model is used to solve the problem of packet delay. The main objective is to provide anonymity and location privacy to defend the potential active attacks without disclosing the node identities using group signature to prevent inside nodes from concluding a real destination using onion routing to improve throughput in the presence of adversary attacks and to reduce the packet loss further by introducing trust management.

II. RELATED WORK

The main focus is to discuss the anonymous communication protocols that have been proposed already for MANETs. Most of the works are based on onion routing protocol in which data is enclosed in a series of encrypted layers to form an onion by a series of proxies communicating over encrypted channels.

Kong and Hong [2] proposed Anonymous On-Demand Routing (ANODR) Protocol is the first one to provide anonymity and unlinkability for routing in MANET. ANODR uses one-time public or private key pairs to attain anonymity and unlinkability but fails to assure content unobservability. An efficient anonymous routing for MANET which provides advantages for ANODR protocol is that routing performance changes notably when different cryptosystems are used to implement the same function. Seys and Preneel [4] proposed Anonymous Routing (ARM) Protocol uses one-time public or private key pairs and go behind only anonymity in route discovery and data forwarding. Yang [5] proposed Discount ANODR performs lower computation and communication complexities at the cost of a small reduction of privacy but provides only source anonymity and routing privacy. Qin [6] proposed On-Demand Lightweight Anonymous Routing (OLAR) scheme which involves the secret sharing scheme which is based on the properties of polynomial interpolation mechanism to reach anonymous message transfer without per-hop encryptions and decryptions. The only job for a forwarder is to perform additions and multiplications which is less expensive than traditional cryptographic operations. Pan and Li [7] proposed Efficient Strong Anonymous Routing (MASR) Protocol which uses onion routing scheme to achieve anonymity but leads to routing overhead and high computational cost. Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks adapts onion routing algorithm to achieve anonymity. In this the node that participates in the protocol, encrypts the whole message with a trust key and says Hello to its preceding nodes within the expiration time. This approach detects the malicious nodes and isolates the node from the network. V-routing based on proactive routing protocol which hides the location and identity of the communication parties but it provides less security for the data. Zhang [9] proposed Anonymous On-Demand Routing (MASK) enables anonymous on-demand routing protocols with high routing efficiency by comparing with ANODR which is very much sensitive to node mobility that may lower routing efficiency. Dong [10] proposed 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 which makes use of one-time public or private key pairs which achieve anonymity and unlinkability. ARMR uses one-time public-keys and bloom filter to find out multiple routes for mobile ad hoc networks and ASR is designed to achieve stronger location privacy, which ensures nodes on route does not have any information on their distance to the source or destination node. Anonymous Location-Aided Routing in Suspicious MANETs uses group signature but this protocols are not suitable for practical approach to routing in mission-critical location-based environment because there is no analysis on protocols performance for privacy and security.

III. EXISTING SYSTEM

In authenticated and anonymous routing protocol for MANETs in adversarial environments the route request packets are authenticated by group signatures, which protect the potential active anonymous attacks without revealing the node identities. The key-encrypted onion routing with a route secret verification message is designed, which records the anonymous routes and also prevent the intermediate nodes from concluding the real destination. The Pseudonymity approach prevents strong eavesdroppers, from exposing local wireless transmitter's identities. Through anonymity the protocol achieves intractability and unlinkability that is tracing ad hoc network packet flows and the relationship among them is prevented. AASR provides higher throughput and lower packet loss ratio in different mobile situations in the presence of adversary attacks. It also provides better support for the secure communications that are sensitive to packet loss ratio. Limitations of the existing system are that the existing protocols are unsafe to the denial-of-service (DoS) attacks, such as RREQ based broadcasting. The feature of unindentifiability and unlinkability are not fully assured. Lack of packet authentication. Difficult for the protocols to check whether a packet has been modified by a malicious node. The problem of packet delay still exists.

IV. PROPOSED SYSTEM

The proposed system uses AASR as well as feature trust management in order to reduce the problem of packet delay and security against the attacks.

Goal of the project is to introduce a new scheme for reducing the package delay of AASR. The new algorithm which is being used is a unified Trust management scheme. The objective is to provide anonymity and location privacy, to provide protection against the active attacks without revealing the node identities using group signature, to prevent intermediate nodes from concluding the real destination using onion routing, to improve throughput in the presence of adversary attacks and to reduce the packet loss.

A. System Overview

In the proposed system where we combine a trust management scheme with the AASR protocol. The nodes move from the destination towards the sink. Through the network it is passed across the AASR protocol and which will result in the nodes with optimized throughput. There are possibilities of the occurrence of errors or problems related to packets which can be solved through the trust model.

In the trust scheme component, the trust evaluation and update module obtains verification from direct and indirect observation modules to calculate and update the trust values. The trust values then are stored in the module of trust repository. Routing schemes in the networking component can initiate secure routing paths between sources and destinations based on the trust repository module. The application component can send data through secure routing paths. As shown in Figure 1.

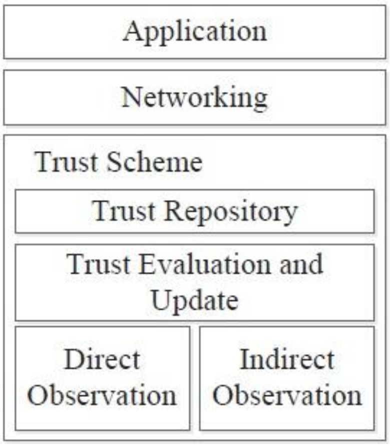

Figure 1 System Overview

B. Trust Management Scheme

In MANET the definition of trust is very much similar to that of the trust meaning explained in sociology. Therefore trust is explained 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 take. Due to the peculiar characteristics of MANETs, trust in MANETs can be characterised into five basic properties: subjectivity, dynamicity, non-transitivity, asymmetry, and context dependency. Subjectivity means that the observer node has the right to decide the trust of the observed node. Dynamicity means the trust of the node should change depending on the etiquette of the node. Non-transitivity shows that if node *A* shows trust on node *B* and node *B* shows trust on node *C*, then it is not necessary that node *A* trust node *C*. Asymmetry shows that if node *A* trusts node *B*, then node *B* does not necessarily trust node *A*. Context-dependency means that trust assessment based on the etiquette of a node. Different facets of actions can be evaluated by different trust. The trust is made up of two components: direct observation trust and indirect observation trust. The two components have been taken into consideration and on these both components the algorithm is generated to find the trust value between the nodes.

C. Trust Calculation with Direct Observation

In direct observation trust, an observer evaluates the trust of its one-hop neighbour on the basis of its own judgement or belief. Therefore, the trust value is the assumption of a subjective probability that a trustor uses to decide whether or not a trustee is dependable or authentic. When a node receives a packet, the number of received packets on account of the type increases by one. If the node forwards the received packet correctly, the number of forwarded packets will increase by one. There are three outlines that the number of received packets will not increase. First, if the packet is lost because of time to live (TTL), the number of received packets will not increase. Second, if a node that receives a packet drops due to buffer overflow. Third a packet is lost due to the poor condition of state of wireless connection.

The following steps are being taken into consideration for Direct Observation:

Step 1 If Node *A* that is an observer node finds that its one-hop neighbour Node *B* is a trustee it receives the packet.
Step 2 the number of packet received then will increase by one.
Step 3 If Node *A* finds that Node *B* sends packet successfully
Step 4 then the number of packets forwarded increases by 1
Step 5 Else if the TTL of the packet becomes zero or overflow of buffer takes place at Node *B* or state of the wireless connection at Node *B* is poor then
Step 6 the number of packets received decreases by one
Step 7 Calculate the trust value and update the old one.

D. Trust Calculation with Direct Observation

In indirect observation from neighbour nodes is used to estimate the trust value of the observed node. Though direct observation from an observer is important in evaluating the trust value of the observed node, the evidence from neighbour nodes are also helpful to decide the trustworthiness of the observed node. Collection of neighbour's views can help in determining whether or not a node is malicious. This mechanism may reduce the inclination from an observer. *A* situation in which a node is amiable to one node but if it is malicious to others it may be diminished.

The following steps are being taken into consideration for Direct Observation:

Step1 If Node *A* that is an observer finds more than one hop neighbours between it and the trustee that is Node *B* then.
Step2 the trust value is calculated.
Step3 Else the trust value is denoted as zero.

E. Mathematical model

1. Defining System
   Let S be the routing protocol S={}
2. Identifying Input
   Identify input S1={N, Pr, Ps ,T,R,SI}
   S={S1,.,...}
   {Ni | i=1,2,3,...}
   where,
   N = Wireless nodes
   Pr= Packets Received
   Ps = Packet Sent
   T = Traffic
   R = Rate of data transfer from node to sink
   SI = Sink Node
3. Identify Input:
   Ni = { Ns , T, R, M}
   R0=max(dist(u,v) | For All $_{v \in}$ N(u))
   where,
   Ns = Network size
   T = Traffic
   R=Radius
   M=Message
4. Identify Control Message Packets
   CTRL
   <source addr, RREQ_ID, dest_addr, hop cnt, route record>
5. Identify Data Packets
   DATA
   <source addr,Data; dest addr >
6. Identifying Process
   Sink node broadcasts RREQ msg to all its neighbors

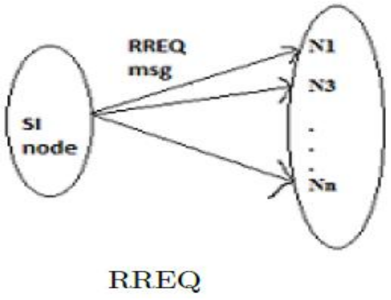

Figure 2 RREQ

7. Identifying Process
   RREQ
   <source addr , RREQ_ID, dest addr,hop cnt,route record >
   source addr , RREQ_ID=uniquely identities
8. Identifying Process
   all nodes return ACK/RERR to Source

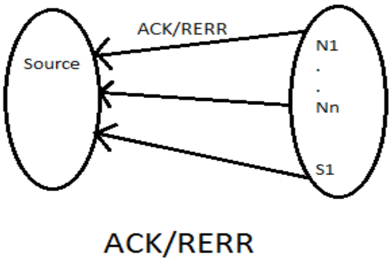

Figure 3 RERR

V. Results

On account of the assumptions the simulation result is being made.

A. Environment Setting

Randomly place nodes in the described area. Each structure has a pair of nodes source and destination with constant bit rate (CBR) traffic .It is assumed that there are two types of nodes in the network: normal node and compromised node. Normal node that follows the routing rules and the compromised node that drop or modify the packets maliciously. It is assumed that the number of compromised nodes is minor as compared to the total number of nodes in the network.

Four performance metrics considered in the simulation: Packet Delivery Ratio (PDR) the ratio of the number of data packets received by a destination node and the number of data packets generated by a source node, *Throughput* the total size of data packets correctly received by a destination node every second, *Average end-to-end delay* the mean of end-to-end delay between a source node and a destination node with CBR traffic, *Message Overhead* the size of Type Length Value (TLV) blocks in total messages

, which are used to carry trust values , *Routing load* the ratio of the number of control packets transmitted by nodes to the number of data packets received successfully by destinations during the simulation.

B. Performance Impovement

The proposed system has higher PDR due to the trust based routing calculation can detect the misbehaviour of malicious nodes. The proposed system with indirect observation has the highest PDR. The number of malicious nodes in the MANET has impact on the throughput of the network. It is assumed that the attackers are independent. Hence, there is no collusion attack in the MANET.

System takes advantage of trust evaluation of nodes in the network so that more reliable routing paths can be established. It is observe that the system with trust can steer clear of malicious nodes dynamically.Therefore, the PDR and throughput are better.

VI. Conclusion

AASR provides higher throughput and lower packets loss ratio in different mobile outlines 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 evaluate the trust values of observed nodes in MANETs.

REFERENCES

[1] Wei Liu and Ming Yu. Aasr: Authenticated anonymous secure routing for manets in adversarial environments. IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. X, NO. Y,, March 2014.

[2] J.Kong and X. Hong, “ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad hoc networks,” in *Proc. ACM MobiHoc’03, Jun. 2003, pp. 291–302.*

[3] J. Kong, X. Hong, and M. Gerla, “ANODR: An identity-free and on demand routing scheme against anonymity threats in mobile ad hoc networks,” *IEEE Trans. on Mobile Computing, vol. 6, no. 8, pp. 888*–902, Aug. 2007.

[4] S. Seys and B. Preneel, “ARM: Anonymous Routing protocol for mobile ad hoc networks,” *Int. Journal of Wireless and Mobile Computing, vol. 3*, no. 3, pp. 145–155, Oct. 2009.

[5] Y. Liu, J. Markus, and W. Susanne, “Discount Anonymous On Demand Routing for Mobile Ad hoc Networks,” in *Proc. 2nd International Conference on Security and Privacy in Communication Networks*,Baltimore, 2006, pp. 1-10.

[6] Q. Yang, H. Dijiang, and K. Vinayak, “OLAR: On-demand Lightweight Anonymous Routing in MANETs,” in *Proc. 4th International Conference on Mobile Computing and Ubiquitous Networking*, Tokyo, 2008, pp. 72-79.

[7] P. Jun, and L. Jianhua, “MASR: An Efficient Strong Anonymous Routing Protocol for Mobile Ad Hoc Network,” in *Proc. International Conference on Management and Service Science*, Wuhan, 2009, pp. 1-6.

[8] R. Song, L. Korba, and G. Yee, “AnonDSR: efficient anonymous dynamic source routing for mobile ad hoc networks,” in *Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN’05), Nov. 2005*

[9] 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.

[10] D. Ying, W. C. Tat, O. K. L. Victor, S. M. Yiu, and C. K. Hui, “ARMR: Anonymous Routing Protocol with Multiple Routes for Communications in Mobile Ad Hoc Networks,” *Elsevier Journal on Ad Hoc Networks*,7(8), pp. 1536-1550, Apr. 2009.

[11] 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.

[12] 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

[13] 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.

[14] B. Yu and M. P. Singh, “An evidential model of distributed reputation management,” in *Proc. ACM AAMAS’02*, (Bologna, Italy), Jul. 2002..

[15] 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