International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

Privacy Protection based on Trust Level of nodes in MANET

T.Azhagesvaran[1], I.Jesintha[2], K.Priya[3], J.Kannadasan[4]

[1,2,3,4]*Assistant Professor, Roever College of Engineering & Technology, Perambalur,India.*

***Abstract*— The disparity with conventional networks, mobile ad hoc networks usually do not provide on-line access to trusted the system or to centralized servers and they exhibit frequent partitioning due to link and node failures. For these reasons, usual security solutions that require on-line trusted authorities are not well suited for securing ad hoc networks. In this paper, we propose trust based an unobservable secure on demand routing protocol that achieves content unobservability by employing secret key establishment based on group signature. The trust based scheme offers a promising approach to avoid wormhole attacks through neighborhood coordination with unlinkability.**

KeyWords – Network security, routing protocol, anonymity, privacy, unlinkability.

Introduction

Compared to wired network, MANETs are much more vulnerable to both active and passive attacks. Wireless transmissions are easy to capture due to the open medium, dynamic topology, lack of centralized monitoring and management points.

To examine the works on securing mobile ad-hoc networks mainly focus on confidentiality, integrity, authentication, availability, and anonymity. There are only a few papers considering the unlinkability and unobservability issues. In order to provide a strong unlinkability and unobservability protection for mobile ad hoc networks, we propose a new scheme namely privacy protection using USOR for mobile ad hoc networks. Unobservability means that the state of item of interest being indistinguishable from any other item of interest at all. The secured routing can be achieved by either content unobservability or pattern unobservability. It is very difficult to take useful information from any transmitted message in both the Cases. Network Security is a concept of protecting data transmission over wireless link. Data Security is the main aspect of secure data transmission over variable network. Data Security is a challenging issue of data communications that touches numerous areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The conventional method of encryption can only maintain the data security, but the information could be accessed by the unauthorized user. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security. So the network security is commonly achieved through the use of cryptography [1].

Mobile ad-hoc network afford multi- hop communication in effect network nodes communicating via other nodes. Mobile ad-hoc network is distinct with characteristics such as purpose-specific, autonomous and dynamic. The rest of the paper is organized as follows. In the next section, we confer related work on anonymous routing schemes for ad hoc networks. Then we describe our unobservable secure on demand routing- trust based scheme and finally, we summarize and conclude the paper.

RELATED WORK

The researchers present a lot of anonymous routing schemes for mobile ad hoc networks in recent years, and they provide various level of privacy protection at different cost. Most of the schemes are mainly based on the public key cryptosystems to achieve confidentiality and unlinkability in routing. ANODR [2] provide anonymity and unlinkability for routing in ad hoc networks, but in this design the unobservability of routing message is not considered. It address two closely related problems namely route anonymity and location privacy. The former case prevents strong adversaries from tracing a packet flow back to its source or destination. The latter case ensures that adversaries cannot discover the real identities of confined transmitters. The major drawback of this method is during the route discovery process, each intermediate node generate a one-time public/private key pair to encrypt/decrypt the routing onion, so as to break the link between source and destination. This paper provides only weak location privacy and route anonymity.

In [3] anonymous secure routing protocol in MANET is proposed. It ensures the security of discovered routes against various active and passive attacks. The unnamed secure routing protocol mainly consists of route request, route response, anonymous data transmission, and route maintenance. An anonymous routing protocol [4] provides a novel anonymous on demand routing scheme for mobile ad-hoc networks. It is an efficient solution that Provides anonymity in a stronger adversary model. An efficient unnamed Dynamic Source routing for Mobile Ad-hoc Networks [5] is proposed to provide three levels of security protection. In [6] Anonymous Routing Protocol with Multiple Routes is proposed for Communications in Mobile Ad-hoc Networks. The main objective is to design a practical trapdoor for anonymous routing. It use symmetric key trapdoor but it must be designed carefully. Symmetric key cryptographic operations usually have better scalability but a public key cryptosystem can offer an efficient way to create secret session keys for the use of symmetric key cryptosystems. The ARMR make use of one time public/private key pairs to achieve anonymity and unlink ability. It has flexibility of creating fake routes to confuse the adversaries and hence increase the level of anonymity. ODAR [7] is based on long term public/private key pairs for anonymous communication. The ODAR protocol provides complete anonymity, source routing path using the bloom filter. It provides anonymity but no unlinkability for mobile adhoc networks, and also it need more computation efforts. In [8] new cryptography concepts called pairing have been implemented.

It allows all the neighboring nodes to authenticate each other without revealing their identities. Here the route request flag is not protected. The main drawback of this method is that setup is quite expensive and key pair depletion attack has present. ALARM [9] makes use of public key cryptography and group signature. The group signature has a good privacy protect feature in which everyone can verify a group signature but cannot identify the signer. But ALARM still leaks lot of sensitive privacy information like network topology, location of node. MOPNET [10] is a mutual anonymity protocol, which enables anonymous query issuance and file delivery for MOPNETs in adhoc environment by employing top secret sharing scheme. The main drawback of this paper is that it does not provide protection from malicious parties. USOR [11] achieves content unobservability by employing anonymous key establishment based on group signature. It comprises of two phases namely anonymous key establishment and route discovery process. Using the unobservable secure on demand routing scheme it is difficult to prevent the network against wormhole attack.

USOR: AN UNOBSERVABLE ROUTING SCHEME

The Unobservable Routing Scheme

The unobservable routing scheme mainly classified into two phases: first one is anonymous key establishment and the second one is route discovery process.

Schemes	Drawbacks
ANODR	Link between the source and destination node is not protected.
ASR	Difficult to cope with active and passive attacks.
ARM	Provide only two level of security protection.
ODAR	Provide only anonymity not unlinkability.
MASK	It cannot protect the route request flag.
ALARM	Privacy information is not secured.
USOR	It cannot prevent the network from wormhole attacks.

Table. 1 Comparison of Anonymous Routing protocol

Anonymous Key Establishment: The node S having the private signing key and private ID-based Key in the network then it follows key establishment procedure as in fig 1. First the source node generates a random number and computes the signature using its private signing key and it broadcast within its neighborhood. Then the neighborhood node verifies the signature in that message. If the verification is successful, neighbor node also generates a random number and computes a signature using its own signing key. The neighbor node computes the session key and replies to S. After getting the reply from

neighbor node, source node verifies the signature and computes the session key. Then it generates the local broadcast key and sends to its neighbor node. The neighbor node receiving the message from source node will compute the same session key then decrypt the message to get the local broadcast key. This is the method for establishing key in USOR.

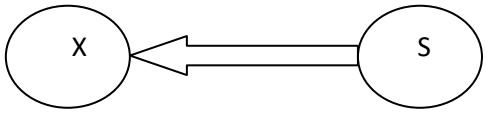


Fig. 1 Anonymous key establishment

Route Discovery Process: The route discovery process mainly comprises of route request and route reply.

Route Request: First the source node chooses a random number and encrypts the information. Then the source node Select a sequence number and another random number, which is used as the index to a specific route. The source node S chooses a nonce to achieve the unobservability. Then S encrypts these messages using its local broadcast key and broadcast the request to its neighbors. Upon receiving the request message from S, the neighbor node tries all its session keys with its neighbors to calculate the pseudonym and find the local broadcast key. Using the broadcast key it decrypts the cipher text then it tries to decrypt the random number using its private ID-based key. If its trial fails then it will act as an intermediate node. Likewise other intermediate nodes do the same as above.

Route Reply: After finding the destination node it starts to send a reply message to the source node. First the destination node chooses a random number and encrypts the information, and then it computes the session key for data protection. After that it generates a new pair wise pseudonym between neighbor node and its own. Finally using its pair wise session key it will encrypt the message and send to its neighbors. When neighbor node receives the message from destination, it finds the sender of the message by manipulative the pseudonym. By using the wise session key it decrypt the cipher text then search the Route table and calculate pseudonym. After the route discovery process the source node can start unobservable data transmission by using the pseudonyms and keys. The main drawback of this unobservable routing scheme is it cannot prevent the network from wormhole attack. So we move towards trust based USOR.

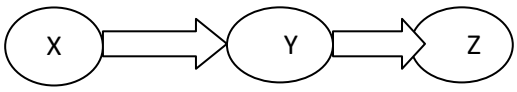
System Model (Trust Based Usor)

The main goal is to design a protocol is to prevent the wormhole attacks in mobile adhoc networks. We detect the wormholes in the system by means of an effort-return based trust model. To set up a wormhole attack, an attacker places two or more transceivers at different locations on a network as shown in figure2 as follows. For correct execution of the model, the subsequent conditions must be met by all participating nodes:

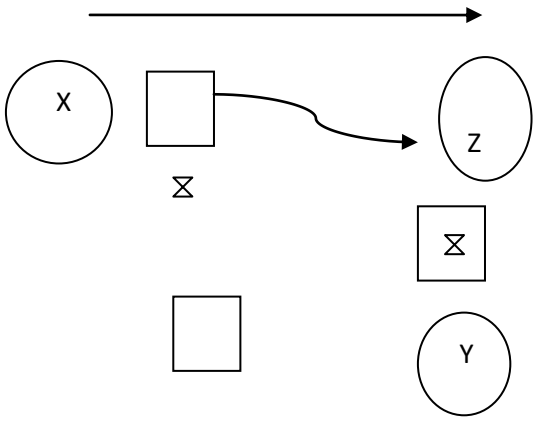
1) All nodes support promiscuous mode operation.
2) Sender and receiver are omnidirectional and that they can receive and transmit in all directions.
3) The transmission and reception ranges of the sender and receiver are comparable.

Each node executing the trust model, measures the exactness and Sincerity of the immediate neighboring nodes by watching their Participation in the packet forwarding mechanism. After the key establishment and routing process we have to measure the trust level for each and every node in the participated route reply process. So based on the trust level we can avoid the wormhole attack present in the networks. Any caring node not able to forward a data packet, due to radio interference, hardware faults, or environmental conditions, is classified as selfish.

Normal Network



Network under Wormhole



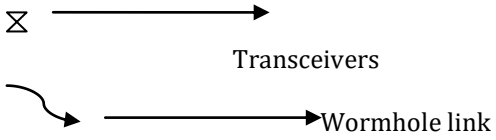


Fig. 2 Set-up of a wormhole

but, in case no other alternate trusted nodes are available, these selfish nodes will be engaged into the routing process. So any node incorrectly forwarding a data packet, by not ensuring its trust level, are classified as malicious and are not included in any subsequent data connections.

Performance Evaluation

We evaluate the performance with the following metrics: Packet deliverance ratio: the ratio of the amount of delivered data packet to the number of packets transmitted towards the destination. This illustrates the level of delivered data to the end.

∑ Number of packet received/∑ Number of packet sent.

Packet delivery delay: The variation in packet delivery delay is called as "jitter". The delay is defined from the initiate of the packet being transmitted at the source on the way to the finish of the packet being received at the destination.

Average node speed: Average node speed is defined as the total reserve traveled separated by the total time it took to pass through this distance.

We apply the trust base USOR in java Net Beans and the simulation is done with 30 nodes. The recreation result of trust based usor method is obtained as shown in fig 3 and 4.

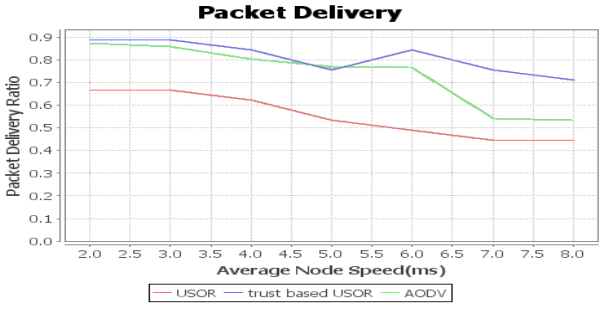


Fig.3. Packet delivery ratio

According to the fig.3 the AODV has better average packet delivery ratio than the other schemes. But in the trust based USOR we can achieve the better packet delivery ratio even in the presence of false nodes than the AODV.

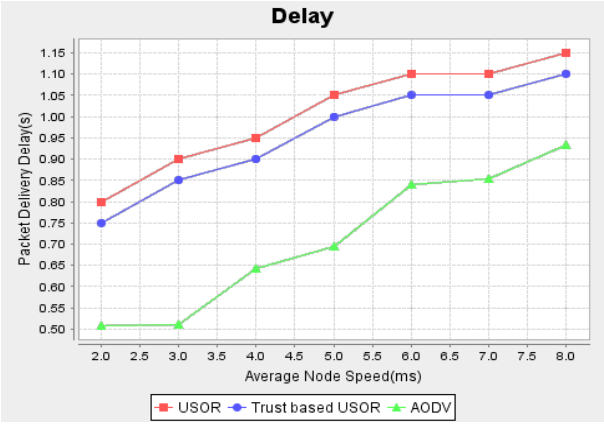


Fig. 4.Packet delivery latency

In fig. 4 the AODV has the least delivery latency but provides low level of security. In USOR the delay is maximum because of that the packet delivery is only through the trusted neighbors and local key construction delay. The main reason of the reduction in packet escape delay for expectation based USOR is that the level of trust is calculated in the route reply process itself.

Conclusion and Future Work

We suggest the trust based USOR to resolution the wormhole attack in MANET environment. Here routing is based on the trust level of nodes which has been calculated in the route reply phase itself in order to reduce packet delivery latency. A packet delivery ratio too high compartively the USOR .Also the performance evaluation shows the better packet delivery ratio and average packet delivery delay. We are working towards an implementation of the same against DoS attack as future work.

REFERENCES

[1] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," in Advances in Cryptology–04, Lecture Notes in Computer Science, vol. 3152, 2004,PP, 41–55

[2] J. Kong and X. Hong, "ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks," in Proc. ACM MOBIHOC'03, pp. 291–302.

[3] B.Zhu, Z.Wan, F.Bao, R. H. Deng, and M. KankanHalli, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102–108.

[4] S.Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks," in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications, pp. 133–137.

[5] L. Song, L. Korba, and G. Yee, "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks," in Proc. 2005 ACM Workshop on Security of Ad-Hoc and Sensor Networks, pp. 33–42.

[6] Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1536–1550, 2009.

[7] D. Sy, R. Chen, and L. Bao, "ODAR: On-Demand Anonymous Routing in Ad Hoc Networks," in 2006IEEE Conference on Mobile Ad-hoc and Sensor Systems.

[8] Y.Zhang, and W. Lou, "Anonymous Communications in mobile ad hoc networks," in 2005 IEEE INFOCOM.

[9] K. E. Defrawy, G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp.1345–1358, 2011.

[10] J. Han, and Y. Liu, "Mutual Anonymity for Mobile Peer- to-Peer Systems,"IEEE Trans. Parallel Distribution Systems. vol. 19, no 8, pp. 1009–1019, Aug.2008.

[11] Zhiguo Wan, Kui Ren, and Ming GU, "An Unobservable Secure On Demand Routing Protocol for Mobile Ad Hoc Networks,"IEEE Transactions on Wireless Communications, Vol.11, NO.5, MAY 2012.

[12] Jesintha.I , Thiraviya Suyambu.G, Priya.K, Azhagesvaran.T "Efficient Broadcast Authentication with Highest life Span in Wireless Sensor Networks" International research journal of Engineering and Technology (IRJET) Volume 2 Issue 9, December 2015.

[13] Priya .K , Jesintha.I, Kannadasan .J, Sivasakthi T, Surya.M, Thiraviya Suyambu.G, "A proficient recognition method for ML-AHB bus matrix. "International research journal of Engineering and Technology (IRJET) Volume 2 Issue 9, December 2015.

[14] Ambiga, S., and M. Ramasamy. "Rural Women Entrepreneurship-A Managerial Perspective." Middle-East Journal of Scientific Research 23.3 (2015): 479-484.

[15] Ambiga, S., and M. Ramasamy. "Women Entrepreneurship Development in India." Jurnal Teknologi 64.3 (2013).

[16] Ambiga, S., and M. Ramasamy. "Rural Women Entrepreneurship–A Step towards Self Contained Economy."

BIOGRAPHIES

Mr.T.Azhagesvaran, M.E., Assistant Professor Department of ECE, Roever College of Engineering & Technology, Perambalur, Tamil nadu, India. My research Interests are Network security & Antenna Design. He has 2 years of teaching experience.

Mrs.I.Jesintha , M.E., Assistant Professor Department of ECE, Roever College of Engineering & Technology, Perambalur, Tamil nadu , India. Her research Interests are Network security & Antenna Design. She has 5 years of teaching experience.

Mrs.K.Priya, M.E.,Assistant Professor Department of ECE, Roever College of Engineering & Technology, Perambalur, Tamil nadu, India. Her research Interests are VLSI & Antenna Design. She has 6 years of teaching experience.

Mr.J.Kannadasan , M.E., Assistant Professor Department of ECE, Roever College of Engineering & Technology, Perambalur, Tamilnadu, India. His research Interests are Wireless Communication & Mobile communication. He has 8 years of teaching experience