Journal Of Harmonized Research (JOHR)

Journal Of Harmonized Research in Engineering
2(4), 2014, 382-390

ISSN 2347 – 7393

Original Research Article

A NOVEL ROUTING PROTOCOL WITH IMPROVED PERFORMANCE FOR MANET IN ADVERSARIAL ENVIRONMENT

K.T.Gowdhami[1], Mr.G.Arul Kumaran[2], S.Fowjiya[3]
[1]PG Scholar, Department of Information Technology
[2]Assistant Professor, Department of Information Technology
[3]Assistant Professor, Department of Information Technology
Vivekananda College of Engineering for Women, Tiruchengode – 637205, India

Abstract: Security issues have been emphasized when mobile ad hoc networks (MANETs) are employed into military and aerospace fields. In adversary environments, Anonymous communications are important for many applications of the mobile ad hoc networks (MANETs) deployed. A requirement on the network is to provide unidentifiability and unlinkability for mobile nodes and their traffics. Eventhough a number of anonymous secure routing protocols have been proposed, the requirement is not fully satisfied. A new routing protocol, i.e., authenticated anonymous secure routing (AASR), to satisfy the requirement and defend the attacks is being proposed in this paper. The key-encrypted onion routing with a route secret verification message, is designed to prevent intermediate nodes from inferring a real destination. Simulation results have demonstrated that the proposed Novel protocol is effective with improved performance when compared with the existing protocols. The salient feature of AASR is that when trust relationships in such among nodes, there is no need for a node to request and verify certificates every time which reduces the computation overheads. Meanwhile, with neighbors' trust recommendations, a node can make objective judgement about another node's trust-worthiness to maintain the whole system at a certain security level.

Keywords- Anonymous Routing, Authenticated Routing, Onion Routing, Mobile Ad hoc Networks

Introduction

In today's fast growing technologies are Mobile ad hoc networks (MANETs) plays an important role with lots of features. They are vulnerable to security threats due to the inherent characteristics of such networks. To provide trusted and secure communications in adversarial environments are difficult, such as battlefields. On one hand, the adversaries outside a network may infer the information about the communicating nodes or traffic flows by passive traffic observation, even if the communications are encrypted. On the other hand, the nodes inside the network cannot be always trusted, since a valid node may be captured by enemies and becomes malicious. As a result, anonymous communications are

For Correspondence:
gowdhami.ktATgmail.com,
Received on: November 2014
Accepted after revision: December 2014
Downloaded from: www.johronline.com

important for MANETs in adversarial environments, the random numbers are used for the nodes identifications and routes are replaced.

The state of being unidentifiable within a set of subjects is defined as Anonymity. In MANETs, the combination of unindentifiability and unlinkability are the requirements of anonymous communications. Unidentifiability means that the identities of the source and destination nodes cannot be revealed to other nodes. Unlinkability means that the route and traffic flows between the source and destination nodes cannot be recognized or the two nodes cannot be linked.

In the past decade, there are many anonymous routing protocols proposed. Our focus is the type of topology-based on-demand anonymous routing protocols, which are general for MANETs in adversarial environments. To develop the anonymous protocols, to anonymize the commonly used on-demand ad hoc routing protocols by a direct method, such as AODV and DSR. For this purpose, the anonymous security associations have to be established among the source, destination, and every intermediate node along a route. The resulting protocols include ANODR, SDAR, AnonDSR, MASK, and Discount-ANODR.

These protocols are also vulnerable to the denial-of-service (DoS) attacks, such as RREQ based broadcasting. Due to the lack of packet authentication, it is difficult for the protocols to check whether a packet has been modified by a malicious node. Recently, group signature is introduced to anonymous routing. In Anonymous and Authenticated Ad hoc Routing protocol (A3RP) the routing and data packets are protected by a group signature. However, the anonymous route is calculated by a secure hash function, which is not as scalable as the encrypted onion mechanism.

Our proposed design of secure routing protocol based on Authenticated Anonymous Routing Protocol(AARP). The proposing the system of framework and network assumptions for the TAARP protocol. The trust model is described. The illustration of TAARP protocol details including routing discovery and maintenance procedures as well as trust recommendation and updating algorithms in II.. Finally we conclude the paper in V.

Related Works

A. Anonymity and Security Primitives

General mechanisms that are widely used in anonymous secure routing.

1) Trapdoor: In cryptographic functions, a trapdoor is defined on a one-way function between two sets .An information collection mechanism in which intermediate nodes may add information elements, such as node IDs, into the trapdoor is called global trapdoor. By the use of pre-established secret keys certain source and certain destination nodes can unlock and retrieve the elements. An anonymous end-to-end key agreement between the source and destination can be possible by the use of trapdoor.

2) Onion Routing: This is a mechanism to provide private communications over a public network. The core of an onion with a specific route message can be set up by the source node. Each forwarding node adds an encrypted layer to the route request message, during a route request phase,. The source and destination nodes do not necessarily know the ID of a forwarding node. The destination node receives the onion and delivers it with the route back to the source. The intermediate node can verify its role by decrypting and deleting the outer layer of the onion.Thus eventually an anonymous route can be established.

3) Group Signature: This scheme can provide authentication without disturbing the anonymity. Each member in a group may have a pair of group public and private keys that are issued by the group trust authority (i.e., group manager). The member can generate its own signature by its own private key, and that signature can be verified by other members in the group without revealing the signer's identity. The tracing of the signer's identity and revoke the group keys can be done only by the group trust authority.

B. Anonymous On-demand Routing Protocols

There are many anonymous on-demand routing protocols. Similar to the ad hoc routing, there are two categories: topology-based and location-based, or in otherwise, node identity centric and location centric. We compare the

protocols in Table I, in terms of the key distribution assumption, node anonymity in route discovery, and packet authentication. The observations are summarized as follows:

First, the routing protocols are designed to work in d-ifferent scenarios. AO2P, PRISM, and ALERT are designed for location-based or location-aided anonymous communications, which requires the localization services. Since ours is for general MANETs, thus focus on the topology-based routing rather than location-based routing.

Secondly, as mentioned in Section I, SDAR, AnonDSR, MASK, and D-ANODR are having problems in meeting the unindentifiability and unlinkability. The node IDs in a neighbor-hood and along a route are possibly exposed in SDAR and AnonDSR, respectively. The plain node IDs are used in the route request of MASK and D-ANODR. In this, we use the node's pseudonym instead of its real ID, to avoid the information leakage during RREQ and RREP processes.

Thirdly, some protocols adopt additional authentication schemes to sign the routing packets, including A3RP, RAODR, USOR, and PRISM. Note that, MASK cannot sign the routing packets although it provides neighborhood authentication,. RAODR provides a master key mechanism, which cannot provide the anonymity, traceability, and enforceability which are supported by a group signature. A3RP and USOR adopt a group signature and use secure hash functions to map the keys and node pseudonyms along a route. The onion based routing is chosen to record the anonymous routes, because the onion is more scalable than other mechanisms and can be extended, for example to multiple paths.

Fourthly, we need to rethink the assumptions on the key distribution and node anonymity in route discovery. For example, ARM assumes that the source and destination nodes share a long-term session key in advance, which is not practical for real-world MANETs. We assume that the nodes are equipped with public and private keys during network initialization phase and can generate the shared symmetric key in an on-demand manner.

Network Scenario

In this section, we present our adversaries and attack models as well as the network assumptions and node model.

A. Network Assumptions

To denote a MANET by T and make the following assumptions.

1) Public Key Infrastructure: 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 $\in\Gamma$), its public/private keys are denoted by K_{A+} and K_A . Similar to the existing secure routing, we assume that there exists a dynamic key management scheme in T, which enables the network to run without online PKI or CA services.

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 $\in\Gamma$), is different for each node. Node A may sign a message with its private key G_A , and this message can be decrypted via the public key G_{T+} by the other nodes in T, which keeps the anonymity of A. We also assume that there exists a dynamic key management scheme working together with the admission control function of the network, which enables the group signature mechanism running properly. Such assumptions are also adopted in the existing work of military ad hoc networks.

3) Neighborhood Symmetric Key: Any two nodes in a neighborhood can establish a security association and create a symmetric key with their public/private keys. This association can be triggered either by a periodical HELLO messages or by the routing discovery RREQ messages. For two nodes A and B (A; B $\in\Gamma$), the shared symmetric key is denoted by K_{AB} and used for the data transmissions between them. There are some approaches supporting the establishment of one-hop shared key, such as MASK, RAODR, and USOR. In this work, we assume one of the approaches is available in T.

The notations are summarized in Table I.

TABLE I
NOTATIONS FOR SECURITY PRIMITIVES

Notations	Descriptions
$^{K}A+$	Public key of node A
^{K}A	Private key of node A
$^{G}T+$	Group public key of network T
^{G}A	Group private key of node A
^{K}AB	Symmetric key shared by nodes A and B
$\{d\}K_{A+}$	Data d is encrypted by key K_{A+}
$[d]K_{A}$	Data d is signed by node A
$d\ K_{AB}$	Data d is encrypted by shared key K_{AB}
$(d)K_{A}$	Data d is encrypted by one symm. key of A
$O_{K}(m)$	Encrypted onion for message m with key K
^{N}A	One-time Nym. generated by A to indicate itself
Dest	A special bit-string tag denoting the destination

B. Node Model

1) Destination Table: Assume that a source node knows all its possible destination nodes. The destination information, including one of destination's pseudonym, public key, and the pre-determined trapdoor string dest will be stored in the destination table. Once a session to the destination is established, the shared symmetric key is required for data encryptions in the session. Such symmetric key is generated by the source node before sending the route requests, and stored in the destination table after receiving the route reply. For example, a sample entry of the destination table is (Dest Nym,Dest String, Dest Public Key, Session Key).

2) Neighborhood Table: Assume that every node locally exchanges information with its neighbors. It can generate dif-ferent pseudonyms to communicate with different neighbors. The neighbours security associations are established as well as the shared symmetric keys. The information is stored in a neighborhood table. For example, a sample entry of the neighborhood table is (Neighbor Nym, Session Key).

3) Routing Table: When a node forwards a route request, a new entry will be created in its routing table, which stores the request's pseudonym and the secret verification message in this route discovery. Such an entry will be marked in the status as "pending". If an RREP packet is received and verified, the corresponding entry in the routing table is to be updated with the anonymous next hop and the status of "active". Meanwhile, a new entry will be created in the node's forwarding table. For example, a sample entry of the routing table is (Req Nym, Dest Nym, V er Msg, Next hop Nym, Status). The timestamp information of the entry can be ignored to simplify the notation.

Protocol Design

In this section, we present the design of NRP protocol. Considering the nodal mobility, take the on-demand ad hoc routing as the base of our protocol, including the phases of route discovery, data transmission, and route maintenance. In the route discovery phase, the source node broadcasts an RREQ packet to every node in the network. If the destination node receives the RREQ to itself, it will reply an RREP packet back along the incoming path of the RREQ. In order to protect the anonymity when exchanging the route information, then redesign the packet formats of the RREQ and RREP, and modify the related processes.

In network, the source node *S* discovers a route to the destination node *D*.

A. Anonymous Route Request

Source Node: Assume that *S* initially knows the information about *D*, including its pseudonym, public key, and destination string. The destination string *dest* is a binary string, which means "You are the destination" and can be recognized by *D*. If there is no session key, *S* will generate a new session key K_{SD} for the association between *S* and *D*.

Dest.Nym.	Dest.Str	Dest. Pub Key	Session Key
^{N}D	*dest*	$^{K}D+$	^{K}SD

Then, *S* will assemble and broadcast an RREQ packet in the format of (1). To simplify the notation, we ignore the timestamp information in the RREQ packet.

$S \rightarrow *$: [*RREQ*; N_{sq}; V_D; V_{SD}; *Onion*(*S*)]G_S (1)

where *RREQ* is the packet type identifier; N_{sq} is a sequence number randomly generated by *S* for this route request; V_D is an encrypted message for the request validation at the destination node; V_{SD} is an encrypted message for the route validation at the intermediate nodes; *Onion*(*S*) is a key-encrypted onion created by *S*. The whole RREQ packet is finally signed by *S* with its group private key G_S .

The combination of V_D and V_{SD} works similarly to the global trapdoor used in ANODR. We introduce V_{SD}:

$$V_{SD} = (N_v)K_v \quad (2)$$

where N_v and K_v are two parameters created by *S* and sent to *D* for future route verification; N_v is a one-time nonce for the route discovery; and K_v is a symmetric key.

The secret message V_D is defined as:

$$V_D = N_v; K_v; dest\ K_{SD}; \{K_{SD}\}K_{D+} \quad (3)$$

If *D* is the receiver of the message, *D* can decrypt the second part of V_D by its private key K_D , and then decrypt the first part by the obtained K_{SD}. Otherwise, the receiver knows that it is not the intended destination.

If *S* and *D* have already established K_{SD} in a previous communication, the costly public encryption in the second part of V_D can be eliminated, and then V_D is defined as:

$$V_D = N_v; K_v; dest\ K_{SD}; pad \quad (4)$$

Where *pad* is a pre-defined bit-string that pads the message to a constant length.

V_{SD} and V_D are separated in the RREQ format (1). For a non-destination node, it can use V_{SD} as a unique identity for the route request.

Now we describe the encrypted onion *Onion*(*S*). *S* creates the onion core as follow:

$$Onion(S) = O_{Kv}(N_S) \quad (5)$$

where N_S is a one-time nonce generated by *S* to indicate itself. The core is encrypted with the symmetric key of K_v, and can only be decrypted by *D* via K_v.

After sending the RREQ, *S* creates a new entry in its routing table, which looks like the following:

Req. Nym.	Dest.Nym.	Ver. Msg.	Next hop	Status
Nsq	^{N}D	^{V}SD	N/A	Pending

2) Intermediate Node: The RREQ packet from *S* is flooded in T. Now we focus on an intermediate node *I*, as shown in Fig. 1. We assume that *I* have already established the neighbor relationship with *S* and *J*. *I* knows where the RREQ packet comes from. The following entries are stored in *I*'s neighborhood table:

Neigh. Nym.	Session Key
^{N}S	^{K}SI
N_J	^{K}IJ

Once *I* receives the RREQ packet, it will verify the packet with its group public key G_{T+}. As long as the packet is signed by a valid node, *I* can obtain the packet information. Otherwise, such an RREQ packet will be marked as malicious and dropped.

I checks the N_{sq} and the timestamp in order to determine whether the packet has been processed before or not. If the N_{sq} is not known in the routing table, it is a new RREQ request; if the N_{sq} exists in the table but with an old timestamp, it has been processed before and will be ignored; if the N_{sq} exists with a fresh timestamp, then the RREQ is a repeated request and will be recognized as an attack.

Then *I* tries to decrypt the part of V_D with its own private key. In case of decryption failure, *I* understands that it is not the destination of the RREQ. *I* will assemble and broadcast another RREQ packet in the following format:

$I \rightarrow *$: [*RREQ*; N_{sq}; V_D; V_{SD}; *Onion*(*I*)]G_I (6)

where N_{sq} , V_D, and V_{SD} are kept the same as the received RREQ packet; the key-encrypted onion part is updated to *Onion*(*I*). The complete packet is signed by *I* with its group private key G_I .

I update the onion in the following way:

$$Onion(I) = O_{KSI}(N_I\ ;\ Onion(S)) \quad (7)$$

Where N_I is a one-time nonce generated by *I* to indicate itself; *Onion*(*S*) is obtained from the

received RREQ packet; this layer of onion is encrypted with the symmetric key K_{SI} .

When *I*'s RREQ reaches the next hop *J*, *J* will perform the same procedures and update the onion in the RREQ with one more layer, which is:

$$Onion(J) = O_{KIJ}\ (N_J\ ;\ Onion(I)) \quad (8)$$

The routing tables of *I* and *J* will also be updated with a new entry as follow:

Req. Nym.	Dest.Nym.	Ver. Msg.	Next hop _	Status
Nsq	N/A	^{V}SD	N/A	Pending

4) *Destination Node:* When the RREQ packet reaches *D*, *D* validates it similarly to the intermediate nodes *I* or *J*. Since *D* can decrypt the part of V_D, it understands that it is the destination of the RREQ. *D* can obtain the session key K_{SD}, the validation nonce N_v, and the validation key K_v. Then *D* is ready to assemble an RREP packet to reply the *S*'s route request.

B. Anonymous Route Reply

1) Destination Node: When *D* receives the RREQ from its neighbor *J*, it will assemble an RREP packet and send it back to *J*. The format of the RREP packet is defined as follow:

$$D \rightarrow *: (RREP;\ N_{rt};\ K_v;\ Onion(J)\ K_{JD}) \quad (9)$$

where RREP is the packet type identifier; N_{rt} is the route pseudonym generated by *D*; K_v and *Onion*(*J*) are obtained from the original RREQ and encrypted by the shared key K_{JD}. The intended receiver of the RREP is *J*.

2) Intermediate Node: We assume that *J* has already established a neighbor relationship with *I*, *D*, and *M*. The following entries are already in *J*'s neighborhood table:

Neigh. Nym.	Session Key _
N_D	^{K}JD
N_I	^{K}IJ
N_M	^{K}MJ

If *J* receives the RREP from *D*, *J* will navigate the shared keys in its neighborhood table, and try to use them to decrypt K_v; *Onion*(*J*) K_{JD}. In case of a successful decryption, *J* knows the RREP is valid and from N_D, and *J* also obtains the validation key K_v. Then *J* continues to decrypt the onion part. *J* knows the next hop for the RREP is N_I .

Then *J* will verify the linkage of the received RREP with its stored RREQ. It tries to use the obtained K_v to decrypt the verification message V_{SD} stored in its routing table. Once *J* finds the matched V_{SD}, it will update the corresponding routing entry as follows:

Req. Nym.	Dest.Nym.	Ver. Msg.	Next hop _	Status
Nsq	N/A	^{V}SD	N_D	Active

Since N_v in V_{SD} is not issued by *J*, *J* is not the source of the RREQ, then it has to assemble another and forward it. The format of *J*'s RREP towards the previous hop *I* is defined as:

$$J \rightarrow *: (RREP;\ N_{rt};\ K_v;\ Onion(I)\ K_{IJ}) \quad (10)$$

Where N_{rt} and K_v are obtained from the received RREP; *Onion*(*I*) is obtained by from the decrypted *Onion*(*J*); the shared key K_{IJ} is obtained from *J*'s neighborhood table. The intended receiver of the RREP is *I*. When the RREP packet travels according to the layers on the onion, it will start at the destination node and move back to its previous node. Each time the intermediate node can associate a value with the underlying wireless link on which the RREP travels, until the RREP packet reaches the source. In our protocol, every node records the one-time link pseudonyms announced by its neighbor node. Then the intermediate nodes' forwarding tables can be established after the RREP's trip.

After *J* updates its routing table, it will also create a new entry in its forwarding table. It may record the multiple paths found in the route discovery. According to the topology in Fig. 1, *J*'s forwarding table may look like the following, in which $N_{X;i}$ stands for the *i*th one-time pseudonyms issued by node *X*:

D issues different pseudonyms $N_{D;1}$ and $N_{D;2}$ to *J*. There are two forwarding relationships at *J*. $N_{I;1} : N_{D;1}$ and $N_{M;1}$:

Rt. Nym.	Pre hop Nym.	Next hop Nym.
$^{N}rt;1$	$^{N}I;$ 1	$^{N}D;$ 1
$^{N}rt;2$	$^{N}M;1$	$^{N}D;$ 2

$N_{D;2}$ describe the two routes of $I - J - D$ and $M - J - D$, as shown in Fig. 1. It can be seen that the forwarding table is made anonymous to any nodes, except for the switching node that owns the table. At the time of being anonymized, the switching relationship at each node en route can also be guaranteed.

3) Source Node: When the RREP packet reaches *S*, *S* validates the packet in a similar process to the intermediate nodes. If the decrypted onion core N_S equals to one of *S*'s issued nonce, *S* is the original RREQ source. *S* will update its routing table as follow:

Req. Nym.	Dest.Nym.	Ver. Msg.	Next hop	Status
Nsq	N_D	^{V}SD	N_I	Active

Then the route discovery process ends successfully. *S* is ready to transmit a data along the route indicated by N_{rt}.

C. Anonymous Data Transmission

Now *S* can transmit the data to *D*. The format of the data packet is defined as follows:

$$S \rightarrow D : (DATA; N_{rt}; P_{data}\ K_{SD}) \quad (11)$$

where *DATA* is the packet type; N_{rt} is the route pseudonym that can be recognized by downstream nodes; the data payload is denoted by P_{data}, which is encrypted by the session key K_{SD}.

Upon receiving a data packet, every node will look into its forwarding table. If N_{rt} in the data packet matches one entry in forwarding table, the node will forward the packet to the anonymous next hop. Otherwise, the data packet will be discarded. Following the similar mechanism as the VCI in ATM network, the data packet can be switched along the route until it arrives at the destination.

D. Routing Procedure

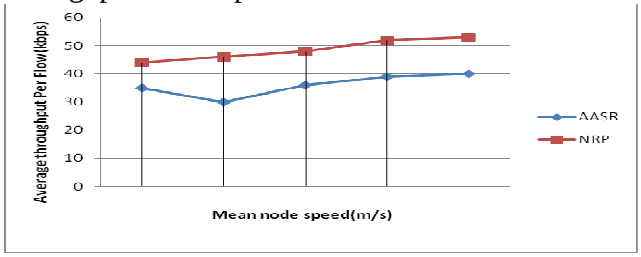
The routing algorithm can be implemented based on the existing on-demand ad hoc routing protocol like AODV or DSR. The main routing procedures can be summarized as follows:

1) During route discovery, a source node broadcasts an RREQ packet in the format of (1).
2) If an intermediate node receives the RREQ packet, it verifies the RREQ by using its group public key, and adds one layer on top of the key-encrypted onion, as (7). This process is repeated until the RREQ packet reaches the destination or expired.
3) Once the RREQ is received and verified by the destination node, the destination node assembles an RREP packet in the format of (9), and broadcasts it back to the source node.
4) On the reverse path back to the source, each intermediate node validates the RREP packet of (2) and updates its routing and forwarding tables. Then it removes one layer.On the top of the key-encrypted onion, and continues broadcasting the updated RREP in the format of (10) when the source node receives the RREP packet, it verifies the packet, and updates its routing and forwarding tables. The route discovery phase is completed.
5) The source node starts data transmissions in the established route in the format of (11). Every intermediate node forwards the data packets by using the route pseudonym.

Simulation Results

Throughput:

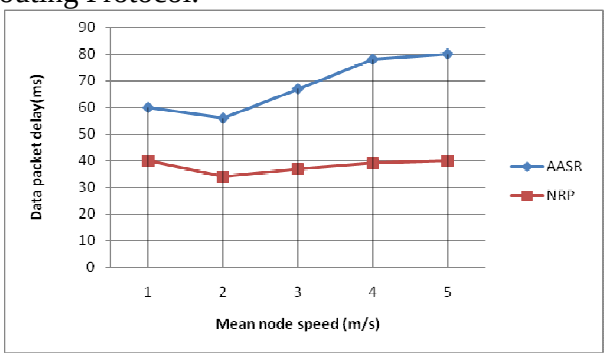
The simulation results are shown below that the novel routing protocols has the performance of the throughput as high when compared to the AASR protocol. The speed is denoted in horizontal axis and its average throughput is in vertical axis. By the graph it notifies the Novel Routing Prototcol has high throughput as compared to AASR.



Performance of the throughput

End-end delay:

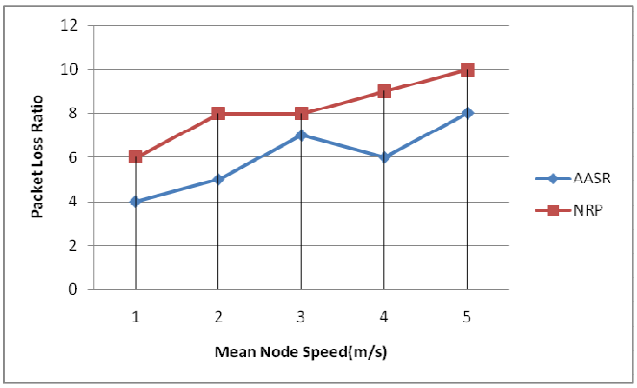
The below graph representation is the end to end delay of the packets that can be possible with the data according to the transfer of data through the Novel Routing Protocol. The minimum of the delay can be occurred. AASR has more delay when compared to Novel Routing Protocol.



End-end delay

Packet Loss Ratio

The packet loss can be minimized with the help of Novel Routing Protocol as compared to AASR.



Conclusion

In this paper, the design of an authenticated and anonymous routing protocol for MANETs. The performance of novel routing protocol can be improved in the adversarial environment. The throughput, packet loss and end-end delay are more advanced in this paper.

In the future we will optimize our trusted routing algorithm and establish some fast response mechanisms when malicious behaviors of attackers are detected. We will also work at applying the trust model into other applications (e.g., key management) and other routing protocols of the MANET (e.g., DSR and DSDV).

References

[1] C. Perkins, E. Belding-Royer, S. Das, et al., "RFC 3561 - Ad hoc On-Demand Distance Vector (AODV) Routing," Internet RFCs, 2003.

[2] D. Johnson, Y. Hu, and D. Maltz, "RFC 4728 - The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," Internet RFCs, 2007.

[3] 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.

[4] 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.

[5] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad hoc Networks," in Proc. IEEE Int'l Conf. Local Computer Networks (LCN'04), Nov. 2004, pp. 618–624.

[6] 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.

[7] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in Proc. IEEE INFOCOM 2005, vol. 3, Mar. 2005, pp. 1940–1951.

[8] 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.

[9] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," in Proc. Int. Conf. on SECURECOMM'06, Aug. 2006.

[10] J. Paik, B. Kim, and D. Lee, "A3RP: Anonymous and Authenticated Ad hoc Routing protocol," in Proc. International Conf. on Information Security and Assurance (ISA'08), Apr. 2008.

[11] 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.

[12] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," in Proc. Int. Conf. on SECURECOMM'06, Aug. 2006.

[13] J. Paik, B. Kim, and D. Lee, "A3RP: Anonymous and Authenticated Ad hoc Routing protocol," in Proc. International Conf. on Information Security and Assurance (ISA'08), Apr. 2008.

[14] S. William and W. Stallings, Cryptography and Network Security, 4th Edition. Pearson Education India, 2006.

[15] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous Connections and Onion Routing," IEEE Journal on Selcted Area in Comm., vol. 16, no. 4, pp. 482–494, May 1998.

[16] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. Int. Cryptology Conf. (CRYPTO'04), Aug. 2004.

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

[18] 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.

[19] R. Song and L. Korba, "A robust anonymous ad hoc on-demand routing," in Proc. IEEE MILCOM'09, Oct. 2009.

[17]M. Yu, M. C. Zhou, and W. Su, "A secure routing protocol against Byzantine attacks for MANETs in adversarial environment," IEEE Trans. on Vehicular Tech., vol. 58, no. 1, pp. 449–460, Jan. 2009.

[18]M. Yu and K. Leung, "A Trustworthiness-based QoS routing protocol for ad hoc networks," IEEE Trans. on Wireless Comms., vol. 8, no. 4, pp. 1888–1898, Apr. 2009.