Security Mandated Analytics based Route Processing with Digital Signature [SMARPDS] - Pseudonymous Mobile Ad Hoc Routing Protocol

K.Vinayakan[1], M.V.Srinath[2]
[1] Department of Computer Applications, STET Women's College, Mannargudi, India
[2] Sengamala Thayaar Educational Trust Women's College, Sundarakkottai, Mannargudi, Tamilnadu, India.

Article Info

Article history:

Received Nov 19, 2017
Revised Jan 21, 2018
Accepted Feb 25, 2018

Keywords:

Analytics
Anonymity
Authentication
Mobile Ad hoc network
Route Processing
Security

ABSTRACT

There are a lot of speculations going on about the interests for privacy in mobile network. Many research works have been proposed in the aspect and these works concentrate more on the anonymity part and there are quite a few implementations of these research works on some applications. Ad hoc routing protocols must have provision for both anonymity providing nature and restriction of information collection from unauthorized nodes. Till recent times, there are a number of ad hoc routing protocols that have been introduced. But, they have lack security features or authentication features or in some cases both. The lack of proper security features leads to a state of vulnerability which at any given point, will act as a threat element. In this paper, we propose Security Mandated Analytics based Route Processing with Digital Signature protocol [SMARPDS]. It is an anonymous and authentication providing routing protocol in Mobile Ad hoc network. In addition, routes are discovered based on analytics done on the node and its present location in the network. SMARPDS provides authentication during the route discovery and transmission process by employing digital signatures on node front and also on packets front.

Corresponding Author:

K. Vinayakan,
Assistant Professor, Department of Computer Applications,
STET Women's College, Mannargudi,
Email: sri_induja@rediffmail.com

1. INTRODUCTION

Ad-hoc is an infrastructure less IP based network environment with absence of centralized environment. Mobile ad hoc networks is known for its property of making each node act as a "router" to forward the traffic to other specified node in the network. In Mobile Ad hoc network, each node will act as both router and host so all nodes have indistinguishable features with similar responsibilities and capabilities and hence it forms a completely symmetric environment [1]. Security in a MANET is considered to be a primary factor requiring attention and anything related to MANET has been viewed from security perspective lately. Recently, as privacy issues are taken into account, a lot of research works about anonymous ad hoc routing protocol have been proposed. The anonymity part discussed in these ad hoc network environment means that the node's location information and the route path information stored in that node must be protected from all threats.

1.1. Mobile Ad-hoc Network (MANET)

A MANET is a peer-to-peer, multi-hop, continuously self-configuring, infrastructure-less, centralized resources lacking, operating without strict top-down network administration mobile wireless network. These properties of the MANETs enable them to out-perform in virtually any scenario of mobile platforms where the data is shared as IP-based information and in environments where the need of physical network infra-structure is impractical. The nodes in the ad hoc network must be in a position to detect and allow communication between its neighboring nodes. Besides that, the currently active node must be able to identify and correlate the type of service that is currently running with its neighboring node. Hence, a mobile ad hoc network's environment is always unpredictable in its network traffic operation and unfixed in relation with the physical topology as the node placement varies depending upon the services offered and communications established. MANET has both fixed and non-stationary network types and the employment of the network type depends on the functional and operational requirements of the topology [2]. There can be many variants of MANET. Consider a mobile communication system network in which a majority of MANETs and nodes equipped with a transceiver at each of its currently active nodes. The combination given by each transceiver is given by the hop of transmitter operating according to a prearranged hopping sequence rate and a wide band reference receiver that has the capability of simultaneously receiving at any given instance of time. The entire operation defined in this process is managed by a centralized system [3]. Some MANET has different implementation in them such as trust based node authentication and communication [4].

1.2. Mobile Ad-hoc Network Attacks and Anonymity

Lack of centralized authentication will lead to different kinds of attacks and if a proper authentication facility is configured, then the anonymity concerns raised. Sometimes the attacks are node based but most of the time, the attacks are detected based on network [5]. Nodes participating in a MANET will be attacked by a malicious node or by attackers taking control over the authentic nodes and prevent it from performing certain tasks. Apart from these factors, other factors like node malfunctioning due to functional failures and loss state of node due to power shortage must also be taken into account. Sometimes these factors too, will be put up by adversaries to create disruption of network traffic. The security mechanism that is carried out must be in a position to withhold all these kinds of node failures [6]. Sometimes these factors apply to every kind of ad hoc networks like mobile social networks and vehicular networks. The kind of ad hoc networks may differ but the methodology of attack mechanism or the sequential flow of data communication between the nodes or node authentication procedures remain the same with respect to the routing protocol established within them.

1.3. Problems of Existing Protocols

Many researchers have proposed many works related to anonymous routing protocols and the way of operation of one protocol differs from the other in a number of ways. When, such protocols are employed in an ad hoc network, the security of the network is directly proportional to the type of network traffic. It handles and the security-related tasks. The following are the list of protocols that have been proposed in relation with the anonymity in MANET.

1.3.1. Anonymous On-demand Routing Protocol (ANODR)

ANODR Protocol for mobile ad hoc networks is deployed in hostile environments. It gives both route anonymity and location privacy factors [7]. Route anonymity is achieved by tracking the packet path from its origination to the destination. It is designed as a routing protocol with broadcast with trapdoor nature. The main problem with ANODR is it is onion routing based. ANODR uses identity free approach, instead of using node identities it uses cryptographic techniques so that only receiver can decrypt the message using its private key [8]. ANODR is purely on-demand routing schemes that set up route as when needed [9]. The main purpose of secure and trust based on-demand multipath routing is to find trust based secure route from source to destination which will satisfy two or more end to end QoS constraints.

1.3.2. On-demand Routing Protocol (ARM)

ARM Protocol is designed for MANET. ARM is a protocol for MANETs that achieves all the anonymity goals while trying to be as efficient as possible [10]. ARM hides routes between sources and destinations, both against dynamic reactive in-action global adversaries and nodes inside the network. ARM employs probabilistic padding and TTL scheme, so the nodes inside the network will not be able to determine whether the node they received a message from is the source of this message or forwarding it. Nor can they tell which nodes is part of a route between two nodes. The RREQ message is formed such that only the destination can recognize that this RREQ was targeted at it, all other nodes can only verify that it was not targeted at them. The source S and destination D shared a secret key kSD and D has a current pseudonym which only d can recognize. Intermediate nodes verify if the RREQ was target to them or not with the help of the pseudonym. The RREP message from the destination is encrypted with the broadcast ID of D.

1.3.3. Family Relationship Routing Protocol (FRRP)

FRRP designed which assigns different relationship and privileges to nodes in the network based on direct and indirect trust by considering resource limitation parameters [11]. FRRP aims at providing common authentication and distributed trust management scheme to MANETs which does not depend on any predefined procedural supposition [11].

1.3.4. Anonymous On-Demand Routing in Mobile Ad Hoc Networks (MASK)

Anonymous On-Demand Routing in Mobile Ad Hoc Networks (MASK) routing protocol is designed than can accomplish communications at both Layer 2 and Layer 3 without disclosing real configuration [12]. It's respective Protocol Data Unit of the participating end points. MASK offered anonymity from both sender and receiver perspective. MASK promotes location anonymity and traffic anonymity.

The existing anonymous routing protocols are not concerned with authentication. If authentication is lacking, then an attacker can unjustifiably operate without any strictness of operation with the route discovery and route location process. These protocols are very weak when it comes to denial of service attacks in which an attacker can make a resource or network unavailable to its intended users. MANET is broadcast based infrastructure-less wireless network so to infect it with a denial of service attack, an attacker can inject more broadcast packets into the existing scheme or re-transmit the existing broadcast packets[12]. When such packets are inseminated into the ad hoc networks, it disrupts the network operations.

1.4. Digital signature

A digital signature is usually some information which is dependent on the message and on data known only to the sender. Secure signature schemes protect the parties involved in the communication [13]. Digital signature schemes are techniques to assure an entity's acknowledgment of having seen a certain digital message. Typically, an entity has a private key and a corresponding public key that is tied to the entity's name (Public Key Infrastructure). The entity generates a string called signature, which depends on the message to sign and his private key [14]. There are several reasons why a signature is compelling [15]: The signature is authentic. The signature cannot be forged. The signature is not reusable. The signed document cannot be altered. The signature cannot be repudiated. The link level congestion occurs when more than one sensor node tries to acquire the channel at same time [15]. In case of link-level congestion, all the nodes attempt to send traffic on the link simultaneously. It results in packet collisions. Furthermore, due to link-level congestion, the link utilization is reduced. To avoid all the above-mentioned effects of congestion, congestion must be controlled or avoided in an effective way. Heterogeneous network have budding to improve network lifetime and also provide sophisticated quality network. Due to limited power battery will exhausted. Thus, energy efficient routing protocol needs to allocate the balance energy burden between the sensor nodes [16].

The anonymity part defined in our work will fall under any one of the five anonymity factors in mobile ad hoc networks.

1. Attribute anonymity: It deals with the identity of the node in the MANET.
2. Route anonymity: It deals with the legitimacy of the route information.
3. Position anonymity: It deals with the layout of the nodes.
4. Packet anonymity: It deals with the integrity of the data that is to be transferred by the nodes.
5. Authentication anonymity: It deals with the authentication part, if created in the ad hoc environment.

Heterogeneous network have budding to improve network lifetime and also provide sophisticated quality network [17]. Due to limited power battery will exhausted. Thus, energy efficient routing protocol needs to allocate the balance energy burden between the sensor nodes [17].The integrated context transport and multicast quick reroute method deployed, and to the standard network mobility management in Mobile-Ad-hoc Network [18].

Researchers have analyzed many works in the area of security in mobile ad hoc networks. Most of the works are concerned with the physical arrangement of the nodes and their respective attributes. There is a clear absence of network traffic monitoring in these networks which leads to bigger problems. Consider a scenario with twenty nodes, each having identical attributes and are capable of transmitting data at the same level as its neighboring nodes. If any malicious nodes gets itself into this network and starts attacking with any one or more of the stated anonymity factors, then the entire topological integrity fails. Now, in such conditions, node authentication plays a very promising role. Node authentication prevents certain attacks and exploits, making the topology secure. But if any authentication procedure is applied, then there is a question of anonymity providence in that network.

In this paper, we propose a routing protocol for ad hoc network which provides anonymity, authentication and accounting factor.

The paper is organized as follows: section 2 explains about our Security Mandated Analytics based Route Processing with Digital Signature protocol [SMARPDS]. In section 3 analyzes the integrity of the proposed algorithm. Finally, section 4 concludes the overall work and the works planned for future extensible factors of this proposed research work.

2. PROPOSED ROUTING PROTOCOL

2.1. Algorithm Working Assumptions

The system assumes that every node in the network has a permanent identity that is known by the other nodes in the network that wish to communicate with this node. Next, we assume that the source [So] and the targeted destination [Dest] share a secret key which is generated and issued by Key Generation Authority which is iterative query based route efficiency controlled (itec-KMA). Itec-KMA handles both the private and public key required for authentication. The private key is not shared with the other nodes. It is used for locally signing the node packets. The public key is openly available and will be used by the nodes that need to validate the signer’s electronic signature. Different mechanisms can be used to synchronize the generated keys used between source and destination (e.g. an encrypted digital signature counter). The destination needs to store two consecutive generated keys, the gkey i that is currently used and the next gkey i+1. The destination advances this window when it receives a Route Request [RREQ] identified with gkey i+1. In order for our protocol to be efficient, we assume that nodes will only share generated keys with a limited set of other nodes. Next, we assume that every node has established a broadcast key with its 1-hop neighborhood. This broadcast key will be used to encrypt the RREP messages.

2.2. System Model Assumption

Proposed protocol needs a centralized key generating and issuing authority, namely Key Generation Authority (itec-KMA). In a Mobile ad hoc network, the receiver node never recognizes its role as to whether it is a transmitting point or it is the intended receiving point. So in this part, we assume that the sender node knows the public key of the destination node. We further assume that each node can efficiently process cryptographic algorithms. Finally, while the network progress, the time clock can be maintained by each node with exceedingly low error rate.

2.3. Conditions Required Achieving Secure Communications

There are some security criteria that need to be achieved in order to establish a secure communication in MANET. These criteria are listed as follows

a. The participating nodes must have an association with each other. In other words, a neighbor relationship establishment is needed. This will ensure node trust ability.
b. The neighbor relationship establishment process must be done with a secure methodology so that confidentiality is maintained which is most needed in sensitive information interchange in the network.
c. Data integrity must be maintained in the network so as to detect corrupted or altered data packets.

2.4. Route Setup

The centralized key generation and issuing authority Key Generation Authority (itec-KMA) handles both the private and public key required for authentication. When a legitimate node (LN) wants to join the network, itec-KMA issues private key (pkey) LN which is used for generating Digital signature (σ) LN ← SIGN pkey LN. And also, itec-KMA informs the time information and its threshold.

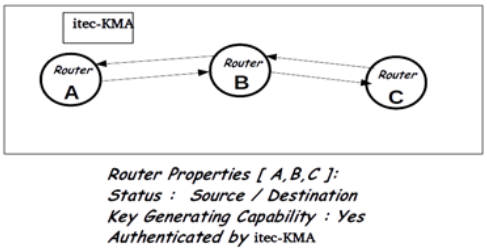
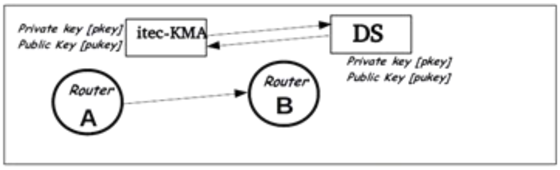

itec-KMA
Router A
Router B
Router C
Router Properties [A,B,C]:
Status : Source / Destination
Key Generating Capability : Yes
Authenticated by itec-KMA

Figure 1. Routing Scenario with Three Routers

The time threshold is determined by communication range of the participating nodes and the transmission speed and thereby it becomes allowance boundary of the timestamp for the participating nodes to decide the freshness of timestamp. All nodes of the network have the group public key (pukey) which is needed to verify the digital signature. The Figure 1 depicts a network environment with three routers scenario.

2.5. Scenario of Event with Respect to Security

In the given scenario, consider that both the routers have the proposed SMARPDS algorithm enabled in them. Consider an event in which Router A is sending a data to Router B with itec-KMA authenticating the entire process of data transfer. There will be four stages in the process namely Route Discovery, Route Selection, Route Authentication and Data Transmission. This scenario is clearly portrayed in Figure 2 with the four stages marked along with the Key Generation Authority (itec-KMA) and Digital Signature (DS) component acting as the part of the routing scenario.



Router A tries to send data to Router B.
Here Router A is the Source (SRC) and Router B is the Destination (DST)
There will be Four States in this Process:
1. Route Discovery 2.Route Selection
3. Route Authentication 4.Data Transmission

Figure 2. Routing Scenario with Two Router Communicating

2.6. SMARPDS Algorithm

In this section, we present a new network protocol called SMARPDS protocol. It is an anonymous and authentication providing routing protocol targeted at Mobile Ad hoc network. The following are some properties of SMARPDS Algorithm:

a) Proper delivery of Packets to the destination (unless hindered by other factors like congestion, downtime.)
b) Efficient data transfer using the fastest and sensible routing method (Analytics based Route Processing)
c) Easy adaptability to Topology change and Network Load factors.

2.6.1. SMARPDS Algorithm-Pseudo ode

In the section, presents the Pseudo code for our proposed network protocol called SMARPDS.

```
BEGIN (SMARPDS algorithm)
    foreach node (nodei)
        *After T seconds send Update messages (UPD_MSG)
        *Receive Update messages (UPD_MSG)
        *Update Routing table
    if(routing table of nodei is not matured)
        Initialize the start and destination node points
        Generate mixed authenticated keys (private and public)
        Generate random keys (private and public) using the DS
        Assign node values and update Analytics table
        Match the keys between itec-KMA and DS
        Use Analytics table
        Update metric values
        Match Route with the Analytics table
            *Broadcast and Update routing table
    elseif(routing table of nodei is partially matured)
        Initialize the start and destination node points
        Generate mixed authenticatedkeys (private and public)
        Match with the existing keys of itec-KMA
        Generate random keys (private and public) using the DS
```

```
          Match with the existing keys of DS
          Assign node values and update Analytics table
          Match existing routes with the newly generated values
          Match the keys between itec-KMA and DS
          Use Analytics table
          Update metric values
          Match Route with the Analytics table
                    *Broadcast and Update routing table
elseif(routing table of nodei is fully matured)
          *Send Update messages (UPD_MSG)
          *Receive Update messages (UPD_MSG)
          Use Analytics table
          Update metric values
          Match Route with the Analytics table
                    *Broadcast and Update routing table
return
end
```

The following Table 1 gives a clear comparison between various other protocols belonging to the same feature set as our proposed algorithm. All of those ensure node anonymity and route anonymity with their built-in set of working architecture. However, this routing protocol does not support location anonymity. Authentication factor is lacking in these protocols.

Table 1. Security Evaluation of Various Protocols

Protocols	Adjunct Characteristics	Route path	Position	Packet	Authentication
ANODR[7]	Yes	Yes	No	No	No
ARM[10]	Yes	Yes	Yes	Yes	No
FRRP[11]	Yes	Yes	Partial	Yes	Partial
MASK[12]	Yes	Yes	Yes	No	No
SMARPDS	Yes	Yes	Yes	Yes	Yes

3. CONCLUSION

The important aspect of Ad-hoc routing protocol is to provide the anonymity. Anonymity with both route and authentication privacy features. Many protocols which operate in MANET environment fail to compensate that level of anonymity and authentication that is required for secure convergence. Lack of authentication means vulnerable model which can create impersonation or falsification of data transferred. The proposed protocol maintains anonymity by generating random keys (private and public) to preserve the authentication of the session between the source and destination after path discovery. In the paper, the proposed a secure ad hoc routing protocol based on digital signature which alleviates the problem of authentication and anonymity perseverance.

In Future work, the same proposed algorithm can be modified and can be made to a complete a defending protocol for MANET with the facility to be less vulnerable and more authentic in its operations.

REFERENCES

[1] Borkar, G. M., and Mahajan, A. R., "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks", *Wireless Networks*, vol. 23, no. 8, pp. 2455-2472, 2017.

[2] Chacko, N.M., Sam, S. and Leelipushpam, P.G.J., "*A survey on various privacy and security features adopted in MANETs routing Protocol*", 2013 International Multi-Conference in Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013, pp. 508-513.

[3] Movahedi, Zeinab, Zahra Hosseini, Fahimeh Bayan, and Guy Pujolle., "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey", *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1287-1309, 2016.

[4] Sharma, G., Mittal, A., and Aggarwal, R., "Attacks on Ad hoc On-Demand Distance Vector Routing in MANET", *International Research Journal of Engineering and Technology (IRJET)*, vol. 3, no. 6, pp. 708- 712, 2016.

[5] Suma, C. C., H. L. Gururaj, and B. Ramesh., "An authenticated encrypted routing protocol against attacks in mobile ad-hoc networks", *Computational Methods in Social Sciences*, vol. 4, no. 2, pp. 5-11, 2016.

[6] Ferrag, Mohamed Amine, LeandrosMaglaras, and Ahmed Ahmim., "Privacy-preserving schemes for Ad Hoc Social Networks: A survey", *IEEE Communications Surveys & Tutorials*, pp. 1-27, 2017.

[7] Jiejun, Kong, and Hong Xiaoyan ANODR, "*Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks*", 4th ACM international symposium on Mobile ad hoc networking & computing, pp. 291-302, 2003.

[8] Padmavathi, G., P. Subashini, and D. Devi Aruna., "ANODR-ECC Key Management protocol with TELNET to secure Application and Network layer for Mobile Adhoc Networks", *International Journal of Distributed and Parallel Systems*, vol. 3, no. 1, pp. 331-339, 2012.

[9] Borkar, Gautam M., and A. R. Mahajan., "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks", *Wireless Networks*, vol. 23, no. 8, pp. 2455-2472, 2016.

[10] Seys, S. and Preneel, B., "ARM: Anonymous routing protocol for mobile ad hoc networks", *International Journal of Wireless and Mobile Computing*, vol. 3, no.3, pp.145-155, 2009.

[11] Ramana, V.V. and Reddy, A.R.M., "Establishing trust between energy aware nodes in MANETs: a family relationship-based approach", *International Journal of Smart Grid and Green Communications*, vol. 1, no.2, pp.114-129, 2016.

[12] Zhang, Yanchao, Wei Liu, Wenjing Lou, and Yuguang Fang., "MASK: anonymous on-demand routing in mobile ad hoc networks", *IEEE transactions on wireless communications*, vol. 5, no. 9, pp. 2376-2385, 2006.

[13] Meijer, Henk, and SelimAkl., "Digital signature schemes", Cryptologia, vol. 6, no. 4, pp. 329-338, 1982.

[14] Sako, Kazue., "*Digital signature schemes*", In Encyclopedia of Cryptography and Security, Springer US, pp. 343-344, 2011.

[15] Shah, D. and Mehta, N., "Method of using text and picture formatting options as part of credentials for user authentication, as a part of electronic signature and as a part of challenge for user verification", U.S. Patent No. 9, 536, 069, 2017.

[16] Tamizharasi, A., Selvathai J.J., Kavipriya A., Maarlin R., Harinetha M. "Energy aware heuristic approach for cluster head selection in wireless sensor network", *Bulletin of Electrical Engineering and Informatics (BEEI),* vol.6, no.1, pp.70-75, 2017.

[17] Manisha R. D., Vemuru S., "Routing Design Issues in Hetrogeneous Wireless Sensor Network", *International Journal of Electrical and Computer Engineering (IJEECS),* vol.8, no.2, pp. 1-10,2018

[18] Aman, A. H. M., Hashim, A. H. A., & Ramli, H. A. M., "Simulation Analysis for Multicast Context Delivery Network Mobility Management", *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol. 5, no. 4, pp. 390-394, 2017.