SEAZOR: A Robust Privacy-Preserving Secure Anonymous Zone Routing in Military Wireless Ad Hoc Networks

Tung Thanh Le, Gil-Won Lee, and Dong-Seong Kim
Networked Systems Laboratory, Department of IT Convergence Engineering, School of Electronic Engineering
Kumoh National Institute of Technology, Gumi, Gyeongbuk 730-701, South Korea
E-mail: {ttungl, skyblue70, dskim}@kumoh.ac.kr

***Abstract*—This paper proposes a robust privacy-preserving secure anonymous zone routing protocol for military tactical networks. Since much of works have been focused on secure anonymous communications in either reactive protocols or proactive protocols, no research has been dedicated to the secure anonymous hybrid routing protocol. In particular, we propose the hybrid routing location-centric communication paradigm that is suitable for privacy-preserving in routing under the hostile medium of the battlefield. The proposed protocol utilizes the features of zone routing protocol plus preserving-privacy which can not only for routes optimization but also for privacy-preserving in secure end-to-end communications in order to prevent the tactical network from attackers. Furthermore, we show the ability of the proposed protocol for efficiently resistance from attackers and compare to the existent techniques to demonstrate the proposed protocol which is outperformed over the military wireless ad hoc networks.**

I. Introduction

Mobile ad hoc networks (MANET) can be quickly deployed to provide robust communications in a variety of dynamic environments. Hence, this feature makes them extremely suitable for a wide range of fields such as supporting for military tactical communications, emergency response efforts, and geographical areas prone to natural disasters. In addition, mobile ad hoc networks can be envisaged to operate over coverage regions with varying node dispersals, node densities, or mobility targets under varying network conditions. Moreover, MANETs deployment scenarios also are concerned with the operations in suspicious mediums, e.g, battlefields. This means that anonymous attacks are either expected or highly possible. Thus, harmful attacks could probably come from both inside and outside of the network, and the results could obviously be unpredictable.

While previous works in secure MANET routing which are concentrated on security problems, little research has been dedicated to privacy issues and combined to efficient routing in it. Note that privacy can be understood with no meaning of communication confidentiality. Instead of that, privacy can be issued to tracking-resistance in military tactical communications [1], [2]. Fig. 1 shows an example of the hostile environment as in the battlefield. A typical terrain is in a mountainous area where military units have been deployed. Some areas of the terrain, military units could possibly be compromised, but such information is known a priori. In order to illustrate clearly as in Fig. 1, an example of military application is as follows. One can figure out that military units could possibly be kept tracking by adversary attacks with different types of nodes, e.g., troops, Humvees military trucks, tanks, unmanned aerial vehicles (UAVs), etc. Hence, adversary attacks could obtain tactical communications and detect the operations command for fighting precisely. Therefore, military units may highly be attacked and destroyed if there is no reliable route which exists through the battlefield.

Most recently, anonymous routing has been studied for MANET with different levels of security and privacy. In [1], the authors constructed one-time pseudonyms used to identify their nodes' locations based on group signatures and location-based mechanism. In the same approach, the authors in [2] proposed an on-demand location-based anonymous MANET routing protocol (PRISM) that are able to prevent the harmful insiders and outsiders. Both of [1] and [2] used the public key cryptography and the group signature for guaranteeing the privacy-preserving [3]. However, while the group signature has an advantage privacy-preserving characteristic, it does not show the identification of the signers. Moreover, the privacy information in [1], [2] are exposed under the nodes' locations and network topology. Therefore, it is needed to be investigated to enhance its characteristics in the network.

Proactive anonymous MANET routing protocols in [4] reports the periodical changes on nodes' pseudonyms and retrieves public keys of each others. Through this feature, the nodes can collect the topology information and maintain communications between nodes. Whereas, reactive anonymous routing protocols show the protect privacy user against both inside and outside attacks as in [3], the wormhole attacks and Denial-of-Service (DoS) attacks are still opening challenges on such protocols.

The purpose of a privacy-preserving feature is to prevent the leakage of information. With an anonymous characteristic, a node could be able to keep its privacy and identity to overcome the inside and outside intrusions from wireless environments [5]. Many researchers have been done such problems through proactive or reactive routing protocols, the privacy-preserving hybrid routing protocols are still an opening challenge for exploiting and utilizing its characteristics. In [6], the author proposed a privacy-preserving routing and incentive protocol

(PRIPO) for preserving the privacy of the users' locations as well as maintaining the source-destination communications by using hashing and symmetric-key-cryptography mechanisms, and unsubscribed receipts. However, this paper does not show the comparison between its efficient performance and previous works, thus, it is unlikable and hardly to be convictive.

In this paper, we focus on two distinguishing issues. Firstly, how to prevent the leakage data from traffic analysis attacks through the routing information, and secondly, dealing with how to design the robust untraceability (tracking-resistance) in military tactical networks based on the privacy-preserving method. In addition, we denote that the term ”privacy-preserving” means preventing adversary nodes from tracking and modification by both inside and outside attacks, e.g., eavesdroppers try to hack the network for tracking nodes or even destroying nodes. The contributions of this paper include: (1) we describe the vulnerabilities of existing routing protocols; (2) we demonstrate the effectiveness of the privacy-preserving secure anonymous zone routing (SEAZOR) protocol for wireless ad hoc networks, in which keeps safe network communications through the robust privacy protection; (3) we compare the SEAZOR protocol to related protocols; that are mentioned in this paper.

The rest of this paper is organized as follows. We describe in detail the SEAZOR protocol in Section III. An analytical security and privacy-preserving are given in Section IV to show how SEAZOR protocol can be applicable as a reliable secure anonymous zone routing protocol through protecting nodes from adversaries. The conclusion summarizes the proposed approach and future work in Section V. Now, we issue the assumptions and goals which involve the features of MANETs' settings, and justify our proposal in the next Section.

II. Problem Formulation

In this section, we discuss about the assumptions, routing protocols selection, adversary paradigm, and goals, which have to approach in the proposed protocol.

A. Assumptions

- A node has its private identity, e.g., address, location, thus, the information exchanged is assumed to attain to privacy between nodes.
- Each node is identified its location based on reasonable precision, e.g., GPS devices [2], or a node is combined the GPS-based and frequency-based technology for efficiency [7].
- Each node is equipped with an appropriate wireless technology depending on the particular circumstances.
- MANET security is assumed that an off-line Trusted Third Party (TTP) will be performed the functions of Certificate Authority (CA) [2]. Before a new node is to be added into the network, it has to make an interaction with TTP to gather its credentials, e.g, public key certificate. Functionalities of TTP consist of distribution as well as monitoring a MANET-wide secret key used for all traffic encryption. It is needed to prevent eavesdroppers who could possibly obtain the information from the intra-communications.

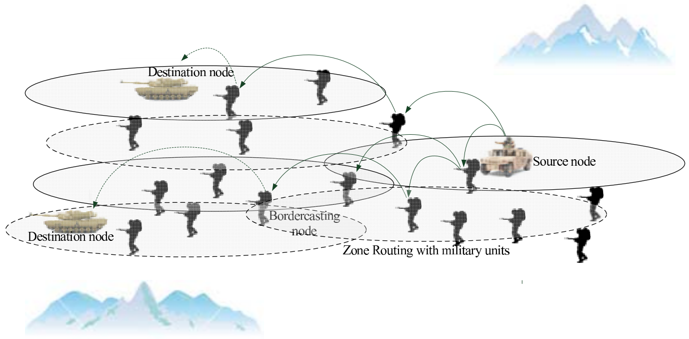


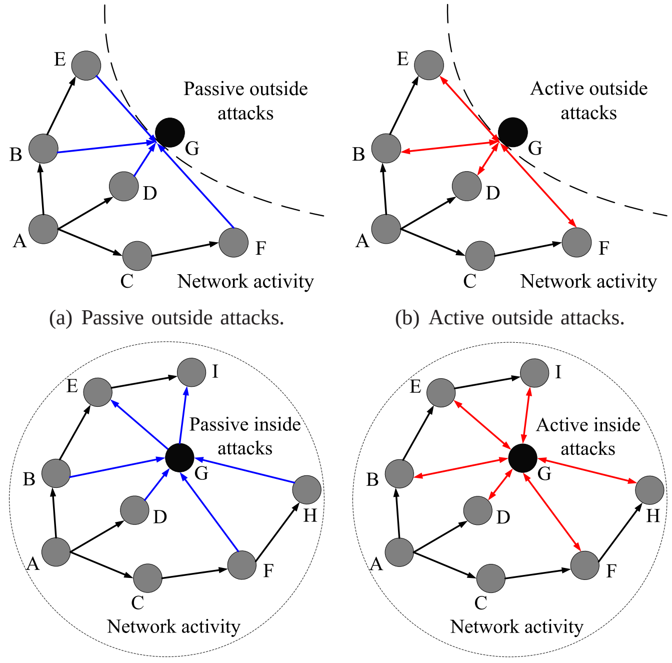
Fig. 1. Zone routing protocol in the battlefield.

B. Routing Protocols Selection

One of the challenges in constructing a MANET is to guarantee the secure routing information for nodes in the network. We can classify the MANETs' routing protocols into three groups: proactive routing (table-driven) protocol group, e.g., OLSR [7], and reactive routing (on-demand) protocol group, e.g., AODV [3], and hybrid routing protocol group, e.g., ZRP [8]. Typically, while proactive protocols work based on the table-driven which contains the information of neighborhood to manage its neighbors, reactive protocols only discover when needed. However, those routing protocols do not take into account any security and anonymity protection, making them vulnerable to various adversary attacks such as traffic injection, track analysis, DoS, and so on [9]. According to a search of secure communications for mobile ad hoc networks, there is the number of secure and anonymous ad hoc protocols which have been done [3], [9], [10], little works have been dedicated on the robust security and privacy-preserving for protecting the routing information from traffic analysis, tracking injection, tracking modification, etc. Therefore, we propose the SEAZOR protocol, which can be able to provide better services from hostile environments in military tactical networks. The SEAZOR protocol utilizes the privacy-preserving plus the zone routing protocol (ZRP), which is a combination of intrazone routing protocol (IARP) and interzone routing protocol (IERP), to protect the MANETs. While IARP is a proactive routing protocol, IERP is a reactive routing protocol, in the ZRP. Unlike other routing protocols, flooding data results in the vulnerability of networks when the routing information could highly be leakage by attacking from adversaries, ZRP minimizes the flooding data in the network by properly changing between the proactive and reactive routing, therefore, it can not only efficiently reduce the routing control traffic, but also minimize the probability of attacks from adversaries for eavesdropping or destroying the network as can be seen in Fig. 1.

C. Adversary Paradigm

Adversary paradigm consists of four typical types of attackers: passive and active outside attacks, passive and active inside attacks. Each kind of attack has a different level of impacts on the network security which is described as below.



(a) Passive outside attacks.

(b) Active outside attacks.

(c) Passive inside attacks.

(d) Active inside attacks.

Fig. 2. The description of different types of attacks.

1) Passive and active outside attackers: The purpose of the passive outside attacker (e.g., node **G**) is to violate either security or privacy or both of them towards nodes inside the network. By compromising privacy, it can be able to eavesdrop all information from communications for purposes, e.g., tracking nodes. While an active outside attacker can change the context of messages and replay messages with harmful information. Thus, the targets of these adversaries can be the disruption of routing or links, phantom nodes, as can be seen in Figs. 2(a) and 2(b), respectively.

2) Passive and active inside attackers: In Figs. 2(c) and 2(d), unlike the passive outside attacker, a passive inside attacker as node **G** receives the information exchanged within the network, then overtly sends non-fraudulent messages without impersonating or modifying nodes' traffic. Technically speaking, the passive insiders are not different from non-malicious nodes as nodes **A–I**, except node **G**, but passive insiders can easily track the other nodes' movements by linking the trajectory information inside the network.

In four types of adversaries, active insiders are the most dangerous adversary type. The active insiders can modify, inject, and reply the messages in communications. In particular, there are two types of the active insiders, consisting of Sybil attacks and locations' fraudulency [1], [11]. A sybil attack creates one or more phantom nodes by generating fake routing control messages or nodes' locations and probably lead to dump the network. Such routing messages contain the authenticated information for security such as signatures, locations' fraudulency that are lying on its own location as a malicious node. Therefore, it can mimic to the attracting locations for traffic routing flows or blinding its own location.

D. Goals

According to the problem which has been abovementioned, we need to solve the problem based on the goals as follows:

- Privacy-preserving – there is no address or public node identity in MANET. Each node is an anonymous identity, including the neighborhood anonymity and routing anonymity. Hence, neighborhood anonymity can not only has the privacy as an anonymous node but also can be authenticated (preserving feature) each other without disclosing its identity [3], [9]. In addition, a node can take advantage of the table-driven in IARP for authentication without other processes such as re-checking the public key. On the other hand, routing anonymity helps the untraceability in the intermediate nodes since they have no clue about source-destination communications such as packet identification, address, etc.
- Security – MANET can be able to resist by a robust protection mechanism from the adversary attacks, consisting of spoofing the IP or MAC addresses, flooding the network, and so on. Thus, ZRP's feature is completely suitable for mitigating such problems by managing nodes in localization with IARP as a group signature.
- Scalability – regarding the latency, it does not increase much when the network is scalable in terms of the routing anonymity.

Therefore, the combination of those features comes out that MANET can be reliable when coping with the attackers in the hostile or suspicious environments, e.g., battlefields.

III. SEAZOR PROTOCOL

In this Section, we propose the SEAZOR protocol that is based on three primary components, including (1) one of the well-known hybrid routing protocols is the zone routing protocol; (2) secure group signatures; and (3) routing information in the IARP's table-driven [8].

A. Zone Routing Protocol

The reason for selecting the zone routing protocol in SEAZOR is thoroughly mentioned in Section II-B. As we can see that proactive protocols, e.g., OLSR [7], can propagate the information in the network by broadcasting data in communications, while reactive protocols, e.g., AODV, are the on-demand routing protocols, thus, there is no need to require the node mobility for synchronization. We take advantage of features from proactive and reactive protocols, we came up with the hybrid routing protocol which is a combination of those protocols that has been studied in [8] plus the privacy-preserving feature to design the SEAZOR protocol as described in Table I.

TABLE I
NOTATIONS

Parameters	Description	Size[bytes]
RREQ	Route request	1
RREP	Route response	1
PK_i, SK_i	Public key, secret key of node i^{th}	128
TS_i	Time stamp of node i^{th}	4
$ZORI_i$	Zone routing information of node i^{th}	~ 8
GS_i	Group signature generated by node i^{th}	~ 200 [2]
H(p)	Hash of package p (e.g., SHA-512)	64
RK	A random session key	$8 \sim 16$
E_{RK}(ZORI)	Encryption of package ZORI with key RK	16
E_{PK}(RK)	Encryption of package RK with key PK	16

B. Secure Group Signatures

Group signatures [12] are basically included by public key signatures and privacy features. According to [2], any member of a group can produce a group signature. Thereby, a group signature can be identified by someone who has a replica of a constant-length group public key. This is to say that a valid group signature is corresponding to the signer, which is the truly member in the group. However, in order to identify the truly signers between two or more valid group signatures in the same or different group members, a group manager has been issued to handle this problem, in which can force open a group signature. It is guaranteed that each member is corresponding to a group member and the off-line TTP (see in Section II-A) is corresponding to a group manager.

C. SEAZOR Features

The design of SEAZOR consists of the authentication of traffic data in source-destination communications without being leakage the information on the intermediate nodes. This means that intermediate nodes have no authority to learn or intervene in the traffic data. Thus, in order to prevent learning or interventing from the intermediate nodes, each source-destination communication has to be encrypted and authenticated via a public key and a secret key. Moreover, the zone routing protocol can be utilized to properly reduce the number of routes instead of broadcasting in proactive protocols and it also increases the monitoring capability in its neighborhood. For instance, a group of military unit needs to be tightly monitoring for cooperative fighting in the battlefield. Therefore, interconnection mechanism of ZRP can be mitigated the computational time of checking security tasks on source-destination communications. Thereby, this feature will be meticulously issued in Section III-D.

D. SEAZOR Operation

The operation of SEAZOR protocol is based on the mechanism of ZRP but including the privacy feature. SEAZOR allows a source node to verify its neighbors through its zone radius area in the IARP, and to specify destination nodes' areas via the IERP. To put simply, we assume that a source-destination communication is consisting of a source node, the intermediate nodes, and a destination node, as illustrated in Fig. 3.

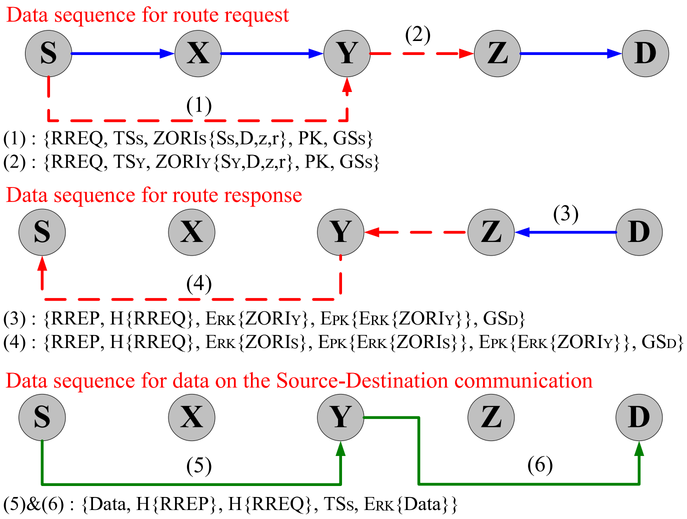

Data sequence for route request
S
X
Y
Z
D
(1)
(2)
(1) : {RREQ, TSs, ZORIs{Ss,D,z,r}, PK, GSs}
(2) : {RREQ, TSY, ZORIY{SY,D,z,r}, PK, GSs}
Data sequence for route response
S
X
Y
Z
D
(3)
(4)
(3) : {RREP, H{RREQ}, ERK{ZORIY}, EPK{ERK{ZORIY}}, GSD}
(4) : {RREP, H{RREQ}, ERK{ZORIs}, EPK{ERK{ZORIs}}, EPK{ERK{ZORIY}}, GSD}
Data sequence for data on the Source-Destination communication
S
X
Y
Z
D
(5)
(6)
(5)&(6) : {Data, H{RREP}, H{RREQ}, TSs, ERK{Data}}

Fig. 3. Data Sequences of the route requests, the route responses, and the source-destination data communication.

1) **Source node S broadcasts a RREQ message**, which includes a route request (RREQ) packet, zone routing information – ZORI (a radius, a source address, a destination address, routes [8]). It also contains a temporary public key – PK_{tempo}, a timestamp of the source node S – TS_{src}, and a group signature – GS_{src}, then calculating all previous works. Unlike the PRISM protocol [2] which just searches its neighbors by iteratively sending RREQs until it obtains its one-hop neighbors, ZORI in SEAZOR can manage the number of neighbor nodes based on the regular zone radius and table-driven routing of each node, thus, it can minimize the latency of the network's adaptation in different network conditions since it does not require to check a group signature. When an adjacent node received a RREQ from its neighbor, a RREQ message is erroneous either if its timestamp is incorrect, or the address of its neighbor node is not listed in the table, or the justification of the group signature is failed. Meanwhile, a received RREP is erroneous if either its timestamp or ZORI or group signature is incorrect. Then, RREPs are logged and the source node will wait until getting another RREP for such this RREQ, otherwise, timeout is occured and the source node will discover the destination node D again. The route request RREQ package is described in (1) and (2) of Fig. 3.
2) **When a node receives a RREQ from its neighborhood**, it will check the validation of TS_{src}. If invalid, the RREQ will be dropped. If this is satisfied, it handles the RREQ hashes by computing a hash of RREQ – H(RREQ). After that, the node continuously checks the ZORI information for recognizing either the destination node is available within its zone or not. If not, this intermediate node caches the H(RREQ) and bordercasts the RREQ to the border nodes for the next hops. If the destination node is available in the routing table of the border node, it then

justifies GS_{src}. If invalid, the RREQ will be dropped, else it stores the RREQ and GS_{src}, simultaneously. At this time, the RREQ message already reached the destination node. Then, the destination node replies a RREP message which consists of H(RREQ), a new random session key – RK, and its ZORI. RK and ZORI are encrypted through PK_{tempo} which is obtained from the RREQ. The group signature of the destination node GS_{dest} also is added into the content of the RREP message. After all, the destination node replies the RREP message to the source node through the forwarding way (from the source to the destination direction) as in Fig. 3.

3) **When an intermediate node receives a RREP**, it will check the corresponding H(RREQ), if it is not satisfied, the RREP message will be dropped. If H(RREQ) is matched, it continuously checks if it contains the source location or not, if it is unsatisfied, the H(RREP) message will be re-bordercasted with H(RREQ) and TS_i to the source node.
4) **When the source node S receives the RREP message**, it verifies the validation of TS_i and the location of the replying node, then justifies the group signature. If it is invalid, the RREP message will be discarded, otherwise, the source node continues to decipher the RK and ZORI which are obtained from the destination node. If the authentication is done, the source node S stores the RREP message and completes the initialization of the route process as in (3) and (4) of Fig 3.
5) **Once the end-to-end communication is established**, the source-destination communication begins to transact the data, including $\{$H(RREQ), H(RREP)$\}$ for the forwarding direction, or for the replying direction with $\{$H(RREP), H(RREQ)$\}$. The purpose of these packages is to justify the routes from source-destination communications, thereby, we can mitigate the information's leakage in communications. After that, the time stamp TS_{src} is added, and finally, the data is encrypted under the random session key [9] before being sent as illustrated in (5) and (6) of Fig. 3.

IV. Security and Privacy Analysis

In this Section, we analyze the security and privacy of the SEAZOR protocol to cope with the attacks as follows.

A. Passive Attackers

1) Outsider: In order to deal with passive outside attackers, the SEAZOR uses a common MANET-wide key to inhibit eavesdropping through the TTP as mentioned in Section II-A.

2) Insider: Passive insiders can be informed by a RREQ about the timestamp of the source TS_{src} and the zone routing information – ZORI. However, TS_{src} just reveals the timestamp of the source, not including the direction of the traffic. Note that a ZORI's RREQ message includes the address of the destination node, while a ZORI's RREP message includes the zone routing of the destination node. Therefore, the passive insider cannot link to RREQs' message since each RREQ contains a unique PK and RK for traffic data encryption and authentication. Moreover, the group signature property prevents whether two or more group signatures which are generated by a same signer, e.g., a passive insider wants to link the RREQs from the same source.

B. Active Attackers

1) Outsider: Active outsiders have been prohibited since all traffic routes utilize a group-wide secret key throughout the network [2]. Thus, it cannot able to modify, replay, or change the messages. In fact, while the timestamp of the RREQ can prevent the replays, each RREP message contains previous RREQ packet that can be able to inhibit the modification of messages. Therefore, the active outsiders hardly obtain the data due to unable to learn the group-wide secret key.

2) Insider: As we know that active inside attacks can cheat about its location and then may reply to the RREQs' messages even though it does not know the ZORI information. Man-in-the-Middle (MiTM) is an example of active inside attacks since it tries to replace a random session key (RK) by its own one, and then it replays the modified RREQs' messages to the network. By this way, MiTM can be able to interpret to the traffic data between the source-destination communications. In order to cope with this kind of attack, an off-line certificate authority (CA) generates each node a number of public key certificates, e.g. RSA. Thereby, each node has one sequence of fixed one-time certificate and the private key [2], thus, the node can be protected from Sybil attacks as mentioned in Section II-C. In addition, group signatures in SEAZOR are implemented to eliminate from the fraudulent locations, e.g., fake GPS locations, which are generated by the attackers.

V. Conclusion and future work

In this paper, a robust privacy-preserving secure anonymous zone routing protocol is proposed based on the group signature and ZORI-based cryptographic system for military wireless ad hoc networks. The proposed protocol utilizes privacy-preserving and zone routing protocol that not only for routes optimization but enhancing the reliability of network communications through the robust privacy protection as well as significantly releasing the computational time through the ZORI's functionality in the proposed protocol. The SEAZOR protocol demonstrated a robust privacy-preserving and can be able to inhibit the attacks from compromised nodes.

From this perspective, we continually study how to prevent from wormhole attacks, DoS attacks that the SEAZOR protocol does not have the functionality for preventing against these attacks. Therefore, the SEAZOR protocol, which is able to overcome these attacks, could be investigated and simulated in the future works.

Acknowledgment

This research was financially supported by the Ministry of Education, Science Technology (MEST) and through the Human Resource Training Project for Regional Innovation 2013.

Algorithm 1 SEAZOR sending algorithm

```
 1: procedure SEAZOR SENDING ALGORITHM
 2:     Initialization a communication
 3:     if Make a communication then
 4:         Obtain the zone routing information ZORI.
 5:         Create and send RREQ.
 6:     else
 7:         Return to Step 2.
 8:     end if
 9:     Checking for RREP.
10:     if Is RREP received. then
11:         Checking a replaying node is in ZORI or not.
12:         if Replaying node within ZORI then
13:             Verifying group signatures
14:             if Group signature is justified then
15:                 Encrypting H(RREQ) and H(RREP).
16:                 Send data.
17:             else
18:                 Log erroneous RREQ.
19:                 Return to checking for RREP.
20:             end if
21:         else
22:             Time-out RREP.
23:             Return to Step 2.
24:         end if
25:     else
26:         Time-out RREP.
27:         Return to Step 2.
28:     end if
29:     Communication established.
30:     Log success RREP.
31:     Completed process of communication.
32: end procedure
```

Algorithm 2 SEAZOR receiving algorithm

```
 1: procedure SEAZOR RECEIVING ALGORITHM
 2:     Check a timestamp for justifying out-of-date or not
 3:     if Timestamp is invalid then
 4:         Log erroneous RREQ.
 5:     else
 6:         Checking for coincident RREQ.
 7:         if RREQ is invalid then
 8:             Log erroneous RREQ.
 9:         else
10:             Checking for node within ZORI from routes table.
11:             if Node is out-of-range then
12:                 Store H(RREQ) into routes table.
13:                 Forward H(RREQ) by bordercasting.
14:             else
15:                 if Group Signature is invalid then
16:                     Log erroneous RREQ.
17:                 else
18:                     Group signatures are justified.
19:                     Create and send RREP.
20:                     Log success RREQ and REP.
21:                     Checking for transacting the data.
22:                     if Checking H(RREQ) and H(RREP) are valid then
23:                         Transacting the data.
24:                     else
25:                         Log erroneous RREQ.
26:                         Waiting for a new communication.
27:                     end if
28:                 end if
29:             end if
30:         end if
31:     end if
32:     Communication established.
33:     Completed process of communication.
34: end procedure
```

References

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

[2] ——, "Privacy-Preserving Location-Based On-Demand Routing in MANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 1926–1934, Dec. 2011.

[3] Z. Wan, K. Ren, and M. Gu, "Usor: An unobservable secure on-demand routing protocol for mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 5, pp. 1922–1932, 2012.

[4] J. Ren, Y. Li, and T. Li, "SPM: Source Privacy for Mobile Ad Hoc Networks," *EURASIP Journal of Wireless Communications Networks*, vol. 2010, pp. 1–10, Apr. 2010.

[5] H. Choi, P. McDaniel, and T. La Porta, "Privacy preserving communication in manets," in *Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Jun. 2007, pp. 233–242.

[6] M. Mahmoud and X. Shen, "Lightweight privacy-preserving routing and incentive protocol for hybrid ad hoc wireless network," in *IEEE International Conference on Computer Communications (INFOCOM) (Workshops)*, Apr. 2011, pp. 1006–1011.

[7] R. Song and C. Peter, "ROLSR: A robust Optimized Link State Routing protocol for military Ad-Hoc networks," in *IEEE Military Communications Conference (MILCOM)*, Nov. 2010, pp. 1002–1010.

[8] Z. Haas, M. Pearlman, and P. Samar, "The zone routing protocol (zrp) for ad hoc networks," *IETF, MANET Internet Draft*, Jul. 2002.

[9] R. Song and L. Korba, "A robust anonymous ad hoc on-demand routing," in *IEEE Military Communications Conference (MILCOM)*, Oct. 2009, pp. 1–7.

[10] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable secure routing for ad hoc networks," in *IEEE International Conference on Computer Communications (INFOCOM)*, Mar. 2010, pp. 1–9.

[11] Y. Hao, J. Tang, and Y. Cheng, "Cooperative sybil attack detection for position based applications in privacy preserved vanets," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Dec. 2011, pp. 1–5.

[12] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *ACM Conference on Computer and Communications Security (CCS)*, Oct. 2004, pp. 168–177.