PASER: Position Aware Secure and Efficient Route Discovery Protocol for Wireless Mesh Networks

Mohamad Sbeiti, Andreas Wolff and Christian Wietfeld
Communication Networks Institute (CNI)
Faculty of Electrical Engineering and Information Technology
Dortmund University of Technology, Germany
Email: {Mohamad.Sbeiti, Andreas.Wolff, Christian.Wietfeld}@tu-dortmund.de

***Abstract*—In this paper we address an acceptable trade-off between security and performance of the route discovery process in wireless mesh networks. We propose a Position Aware Secure and Efficient reactive hierarchical Route discovery protocol (PASER). The proposed protocol is tailored for rescue and emergency operations and aims to combat unauthorized nodes of joining the network or manipulating the route look-up process. In addition, it deals with efficiency and real-time capability requirements in such environments. From a security perspective, the novelty of PASER is the combination of digital signature with lightweight authentication tree and symmetric block cipher to secure routing messages. Another key feature is the support of nodes' geo-positions to increase the security while enabling an advanced network management. Apart from that, PASER treats the network in a hierarchical way and establishes the route discovery process to a large extent upon reactive unicast messages. PASER is generally applicable, as it does not make restrictive assumptions on the network nodes. It provides generic metrics for the constituent links of the discovered routes, allowing the implementation of any route selection algorithm. As a result, PASER enables secure and efficient routing in a wide range of wireless mesh network applications.**

***Keywords*-Secure routing protocols; wireless mesh networks; emergency and rescue operations.**

I. INTRODUCTION

Wireless Mesh Networking (WMN) is an emerging technology, which is receiving increased attention as a high-performance, low-cost and rapid deployment solution for next generation wireless communication systems. A WMN is defined as a dynamic, self-organized and self-configured wireless multi-hop network, consisting of gateways, mesh routers and mesh clients. Gateways and mesh routers build the network backhaul and are responsible for client data transmission. Typically, gateways provide connection to the Internet, whereas mesh routers are responsible for setting up and maintaining the ad hoc network routes. Due to its ubiquitous architecture and wireless transmit channel, it is possible though that mesh routers deviate from the protocol definition and exhibit malicious behavior. The challenge is to prevent such nodes, which we term attackers, from misleading other nodes that a path is better than it actually is. If successful, an adversary can attract network traffic and degrade or disable the communication of other nodes, which might be very crucial in many WMN applications.

Rescue and emergency operations, for instance, is a WMN application field addressed by the research project SPIDER [1], where rescue fighters deploy an ad hoc incident network using dropped units [2]. These operations are very time sensitive and dangerous minds might be on board. Without a satisfactory level of security, terrorists or benefiting organizations may try to disrupt the communication route between rescue fighters and the Command and Control System (CCS). They might try to inject fraud packets to falsify CCS decisions or create a routing black hole, which attracts and sniffs data packets, where any release of such sensitive data could cause a mass hysteria across countries.

Thus, one of the fundamental challenges of the WMN technology is the design of a route discovery protocol that can efficiently establish accurate routes in presence of attackers. Hereby, it needs to deliver data packets between mobile clients with minimum communication overhead, low end-to-end delay and high throughput.

The rest of this paper is organized as follows: Section II reports on related work. Section III presents a review on security threats in WMN and outlines the needed security characteristics to secure routing protocols. In Section IV, PASER is demonstrated, where in Section V its security and performance are discussed. Finally, in Section VI we conclude the paper and give some outlook for future work.

II. RELATED WORK

Most WMN mesh routers nowadays, e.g., HiMoNN [3], are built upon routing protocols designed by the IETF MANET working group: AODV [4], DYMO [5] and OLSR [6]. These protocols along with a plenty of other MANET routing protocols can not be fully applied in WMN for the following reasons:

1) They are designed without having security in mind. Retrofitting pre-existing cryptosystem (e.g., IPsec) to secure them is inefficient. These cryptosystems impose huge overhead and processing delay, hence affecting strongly the overall performance.
2) They deal with the network as a flat network, which is absolutely reasonable in MANET. Thereby, they do not consider the different roles of WMN nodes, namely, mesh routers and gateways. Thus, these protocols are not able to take advantage of WMN characteristics, i.e., most data flow is destined to the gateway (e.g., from rescue fighters to officer in charge).

Many security solutions to secure routing in MANET have been recently proposed, however most of them comprise

 ISBN: 978-1-61208-010-9

either high computational complexity [7] or impose a lot of configuration and management [8] or are still vulnerable to several attacks [9][10][11].

To exploit the WMN characteristics, IEEE has been discussing since 2003 the release of the IEEE 802.11s standard, which deals with hierarchical mesh networks. The current draft has defined a routing mechanism for WMN and termed it Hybrid Wireless Mesh Protocol (HWMP) [12]. However, security in routing or forwarding functionality is not specified in that standard. The protocol does not provide any authentication and integrity of routing messages. Apart from that, HWMP as well as many protocols applied in WMN incorporate a proactive part [13]. Though this part is essential to keep the route to the gateway valid, it is very resource consuming and is always active even when it is not necessary.

In PASER, we address the latter point by adopting the reactive route discovery method with two differences:

- Mesh routers are always responsible for maintaining a route to the gateway. This brings the same advantage as a proactive part in hybrid protocols while using the resources only when needed.
- Route requests are forwarded, when possible, in a unicast manner rather than flooding them blindly, as in conventional on-demand route discovery methods.

From a security point of view, PASER provides a novel hybrid scheme, a combination of asymmetric and lightweight symmetric cryptography, to secure route discovery messages. This novel combination yields a huge performance gain while providing a very high security level. Apart from that, PASER supports the exchange of geo-positioning, hence mitigating a wider range of attacks and facilitating the network management.

III. Security Vulnerabilities in WMN Route Discovery

As mentioned before, PASER's main target scenarios are disaster rescue and relief operations. In such environments, safeguards are indirectly applied to the nodes preventing their compromise, e.g., nodes are mounted on fire brigades tubes. Thus, internal attacks, where nodes from within the network are involved, are a less realistic threat in these environments, whereas external attacks, which are performed by illegitimated nodes, are of paramount importance. The latter class of attacks essentially aims to violate the reliability of the network and the availability of its services. The most relevant attacks of this class with respect to the route discovery process are listed below:

Impersonation attack: Using MAC and IP spoofing, an attacker fakes the identity of authorized nodes and thereby joins the network. The attacker can then carry out all types of insider attacks - *the lack of proper authentication of nodes is the main reason for the success of impersonation attack.*

Location disclosure attack: This attack reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and attempts to learn the network traffic pattern. By analyzing changes in the traffic pattern, attackers try to figure out the identities of communication parties and plans further attack scenarios - *the lack of anonymity and confidentiality of routing information is the ground of this attack.*

Malign attack: An attacker blackmails an uncompromised node, causing other nodes to exclude it from the network, thus, prohibiting that node to exchange data - *a weak node revocation mechanism is the essential reason of the network vulnerability to such an attack.*

Man-in-the-middle attack: An attacker impersonates a sender and a receiver by establishing independent connections to them and making them believe that they are talking directly to each other. The success of such an attack gives the attacker a full control of the entire conversation. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, an attacker within reception range of two nodes, can insert himself as a man-in-the-middle). A man-in-the-middle attack can only succeed when the attacker can impersonate each endpoint to the satisfaction of the other - *weak mutual authentication is the main reason for the attacker's ability of man-in-the-middle attack.*

Replay attack: An attacker records another node's valid control messages and resends them later. First, this causes other nodes to update their routing table with stale routes. Second, unnecessary packets are processed and forwarded within the network. The latter, also known as resource consumption attack, targets to consume network bandwidth and node battery power - *the main reason of the network vulnerability to such attack is the lack of adequate packet freshness verification mechanism.*

Tempering attack: An attacker forges routing packets generated by legitimated nodes (e.g., tempering sequence number or metric of packets) and hence causes wrong routing decisions like redirection through suboptimal routes or route loops. This attack causes severe degradation in network performance - *the fundamental reason of the attacker's ability of tempering the routing information is the lack of packet integrity check.*

Wormhole attack: A pair of attackers, linked via a fast transmission path (tunnel), forward route requests more quickly than legitimate nodes. The tunneled packets can propagate faster than those through a normal multi-hop route. This causes victim nodes to always use the tunneled route to transmit their packets. The latter enables the attackers to gain information about specific communication traffic in the network or selectively forward packets. The attacker could even prevent the discovery of any routes other than through the wormhole - *the lack of authentication of transmissions between neighboring nodes in the route discovery is a main issue with respect to this attack.*

Thus, in order to combat the aforementioned attacks and to mitigate their risk to a large extent, a secure route discovery protocol has to fulfill the following security goals:

 ISBN: 978-1-61208-010-9

1) Anonymity
2) Message confidentiality
3) Message freshness and integrity
4) Neighbor transmissions authentication
5) Node authentication

The first goal is only necessary to combat location disclosure attack. We didn't consider this goal while designing PASER for the following reasons:

- The location and role of nodes in environments such as disaster rescue and relief operations are to a large extent known and hence protection against this attack is not really required.
- The performance cost of achieving the anonymity goal is very high and we are seeking a good trade-off between security and performance.

IV. The PASER Protocol

In this Section, we describe the main components of PASER.

A. PASER Objectives

PASER is an efficient secure route discovery protocol for wireless mesh networks. It is a mechanism that provides a route to a node (mesh router or gateway) wishing to send a packet to a destination. Hereby, PASER asserts that the discovered route is accurate in terms of metric and legitimized nodes in the presence of external attackers. Moreover, it keeps the consumption of network resources minimal. That is, PASER aims to ensure the reliability of the network and the availability of its services in an efficient manner.

From security point of view, PASER has to fulfill the following goals: Message confidentiality, message freshness and integrity, neighbor transmissions authentication and node authentication. Message confidentiality is only used where PASER is vulnerable against man-in-the-middle attacks. From performance point of view, PASER aims to strongly decrease the number of messages it exchanges over the network and to keep the cost of its security mechanisms minimal. To achieve these goals, we consider the following assumptions in the given priority:

1) Only legitimated nodes hold a valid certificate.
2) Nodes feature low mobility.
3) GPS signals are available at the application scene and nodes incorporate a secure GPS device, i.e., received GPS information is secure in terms of integrity and authenticity.

B. PASER Cryptographic Primitives

In this Subsection, we describe how the main security building blocks of PASER are applied.

1) Digital Signature Scheme: PASER specifies to apply a digital signature on its broadcast-messages. This signature is mainly necessary to guarantee the authenticity of these messages and thereby to establish trust between one hop neighbors. We recommend any of the standardized algorithms in [14]. The key pair used by the algorithm is the one bounded to the node identity in his certificate.

2) Symmetric Block Cipher: PASER prescribes the use of symmetric block cipher to encrypt its unicast-messages. This encryption is mainly necessary to protect these messages against man-in-the-middle attacks within a short time interval after sending them. The key used by the cipher is a group key distributed to the nodes during the setup phase of the network. The selection of the block cipher depends on the application of PASER and therefore it is left open. We recommend however the usage of the lightweight block cipher PRESENT [15]. PRESENT was specifically designed with constrained applications such as passive low-cost RFID-tags in mind. PRESENT is a simple substitution-permutation network with a block size of 64 bits and two different key sizes: 80 or 128 bits. We recommend the version with an 80 bit key for PASER since here we are seeking short-term security.

3) Authentication Tree: An authentication tree [16] is a complete binary-tree equipped with a hash function and an assignment function F such that for any interior node n_{parent} and two child nodes n_{left} and n_{right} the function F satisfies: $n_{parent} = F(n_{left}, n_{right}) = hash(n_{left}||n_{right})$, with $||$ denoting concatenation. The hash function to be used should be practically secure and efficient, such as SHA-256 or the winner of the SHA-3 competition [17]. We use authentication tree in PASER to build from hash functions an lightweight secure authentication scheme between one hop neighbors. Figure 1 illustrates an example of this approach.

Each node generates 2^n secrets, where n is a configuration parameter and is determined based on the application of PASER; these secrets are the leaf pre-images of the tree. Each leaf node is a hash of these secrets and each internal node is the hash of the concatenation of two child values. After computing root, a node (Alice) publishes that root to its one hop neighbors (Bob). A node can then authenticate itself to a neighbor by disclosing one secret, e.g., $Secret1$,

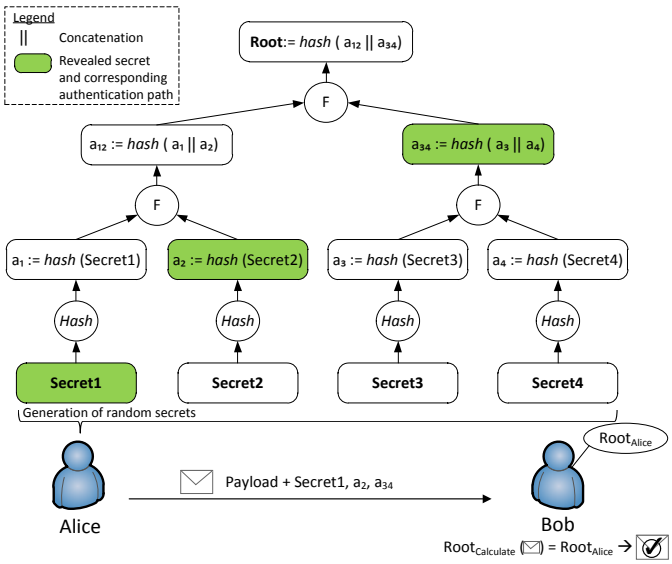

Figure 1. Authentication Tree Application

Table I
PASER MESSAGES

Name	Notation
Untrusted Broadcast Route Request	UB-RREQ
Untrusted Unicast Route Reply	UU-RREP
Trusted Unicast Route Request	TU-RREQ
Trusted Unicast Route Reply	TU-RREP
Trusted Unicast Route Reply-Acknowledge	TU-RREP-ACK

and sending it along with its authentication path, a_2 and a_{34}, see Figure 1. The authentication path of a secret consists of values of all the siblings of the secret corresponding leaf on the path between that leaf and the root. To verify the disclosed secret a receiver needs to compute the potential values of its ancestors by iteratively using of the F function. A secret is authenticated and accepted as correct if and only if the computed root value is equal to the already known root value of the node.

PASER tree secrets are l bits long, where l is a configuration parameter and $l > n$. A secret shall be constructed as specified in Figure 2.

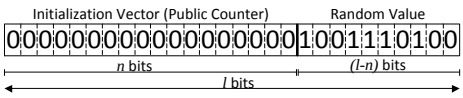

Figure 2. Authentication Tree Secret Construction

The least significant $(l - n)$ bits are generated randomly for each secret. The most significant n bits constitute an initialization vector, the value of which is 0 for the first secret. The initialization vector is then incremented by one by each subsequent secret. When the maximum value $(2^n - 1)$ is reached, a node must generate a new root. The latter asserts the freshness of a secret. That is, a secret value can never be used twice for a given root. This technique is used to prevent replay attacks.

C. PASER Messages

PASER differs between messages destined to new neighbors and messages addressed to already known, trusted neighbors. From security perspective, messages addressed to new neighbors comprise identification fields that aim to establish a trusted relationship. These messages are always signed and their name is always prefixed with *U*, which stands for untrusted. Messages sent to trusted neighbors just include authentication fields to confirm the identity of the sender. These messages are always encrypted and their name is prefixed with the letter *T*, for trusted. PASER comprises five types of messages as depicted in Table I.

Table II (see next page) depicts the fields which constitutes these messages,

where * denotes fields that are included in a message if and only if the gateway flag *GFlag* is set. *Seq* is a concatenation of message type and node ID, where ID matches a sequence number in [4]. The address range list indicates all the addresses a node is responsible for. The latter is necessary in case of multiple interfaces. It allows the declaration of all node interfaces that participate in another routing domain. This is necessary in WMN since mesh routers mostly comprise at least two interfaces.

D. PASER States

In PASER, a node can be in two different states as illustrated in Figure 3.

At power-up the node enters the *UNREGISTERED* state. In this state the node is not known to the network. Before any communication can take place, it undergoes the following steps in the given order:

1) It generates empty routing and neighbor tables according to Table III. Hereby, a neighbor table comprises the position field if and only if the node is mesh router. In contrast, this field is included in the routing table by a gateway, because a gateway in PASER has knowledge of the position of all nodes. The neighbor Flag (*NeighFlag*) reflects the trust relation between a neighbor and that node.
2) It computes a hash tree root element and depending on the node type it executes the following:
   Gateway: It requests a random group key from a key distributing center (KDC). The physical location of the latter is less significant. For instance, in emergency and rescue operations it is reasonable to install the key distribution center as a web service at the CCS. Typically, gateways are placed near to the fire-fighting command and control vehicle and have a stable Internet link to the KDC, e.g., via satellite.
   Mesh router: It starts a route discovery for a gateway. To augment the security of this step, gateways may be assigned with the role "*gateway*" in their certificates.
3) It requests a certificate revocation list from a certificate authority and enters the registered state. We do neither restrict the choice of the protocol used to request the

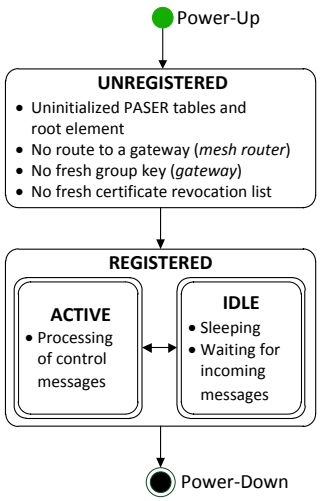

Figure 3. Node Lifetime State Machine

Table II
MESSAGE CONTENT DECLARATION

Field	UB-RREQ	UU-RREP	TU-RREQ	TU-RREP	TU-RREP-ACK
Basic fields					
Message type	✓	✓	✓	✓	✓
Querying node	✓	✓	✓	✓	✓
Destination node (*Dest*)	✓	✓	✓	✓	✓
Sequence number (*Seq*) of querying node	✓	✓	✓	✓	✓
Destination node gateway flag (*GFlag*)	✓	✓	✓	✓	
Address range list (*AddL*) of forwarding node	✓	✓		✓	
Route list from querying node to forwarding node	✓	✓	✓	✓	
Metric for the route between querying node and forwarding node	✓	✓	✓	✓	
Metric for the route between destination node and forwarding node		✓		✓	
Neighbor (Neigh) identification fields					
Certificate (*Cert*) of querying node	*		*		
Certificate of forwarding node	✓	✓			
Root of forwarding node	✓	✓			
Initialization vector (*IV*) of forwarding node	✓	✓			
Geographical position (*Geo*) of querying node	✓	✓	*		
Geographical position of forwarding node	✓	✓			
Encrypted group transient key (*GTK*)		*		*	
Signature (*Sign*) of forwarding node	✓	✓			
Neighbor authentication fields					
Secret (*Sec*) of forwarding node			✓	✓	✓
Authentication path (*Auth*) of forwarding node's secret			✓	✓	✓
Hash of message fields			✓	✓	✓

revocation list nor the location of the certification authority. At this stage of the network setup, it is assumed that also the mesh routers have a stable route to the CA/KDC, since they are typically turned on before disposing them (near to the gateways), thereby, they have a very good connection to the gateways. For the secure und fast communication between the mesh nodes and the CA/KDC we proposed in [18] an efficient single sign-on solution called Role integrated Certificate-based Single Sign-On (RC-SSO). This solution is based on the SSL/TLS communication procedure with certificates. Hereby, the certificates are integrated with roles, which reflect predefined mesh nodes' type (either router or gateway). Simulation and experimental results show that RC-SSO outperforms the widely spread Security Assertion Markup Language (SAML) by up to 80 %- *Implementing this solution makes PASER robust, among others, against malign attacks executed on the communication link to the CA/KDC.*

The *UNREGISTERED* state is mainly a state used at power up. Once the node has registered with the network, it is typically in one of the two sub-states, *ACTIVE* or *IDLE* of the *REGISTERED* state. *ACTIVE* is the sub-state where the node is active with transmitting and receiving PASER messages. *IDLE* is a low activity sub-state in which the node sleeps in order to reduce battery consumption. Note that a mesh router in *REGISTERED* state must always maintain a route to a gateway. That is, when the route to the gateway is not valid anymore; it has to restart a route discovery for the gateway.

Table III
ROUTING AND NEIGHBOR TABLE FORMAT

Routing Table						
AddL	Dest	Seq	GFlag	Cert	NextHop	Metric
Neighbor Table						
	Neigh	NeighFlag	Root	IV	Position*	

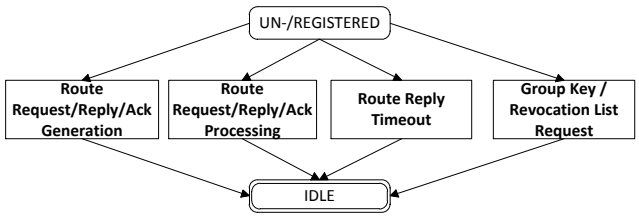

Figure 4. Node Lifetime Operations

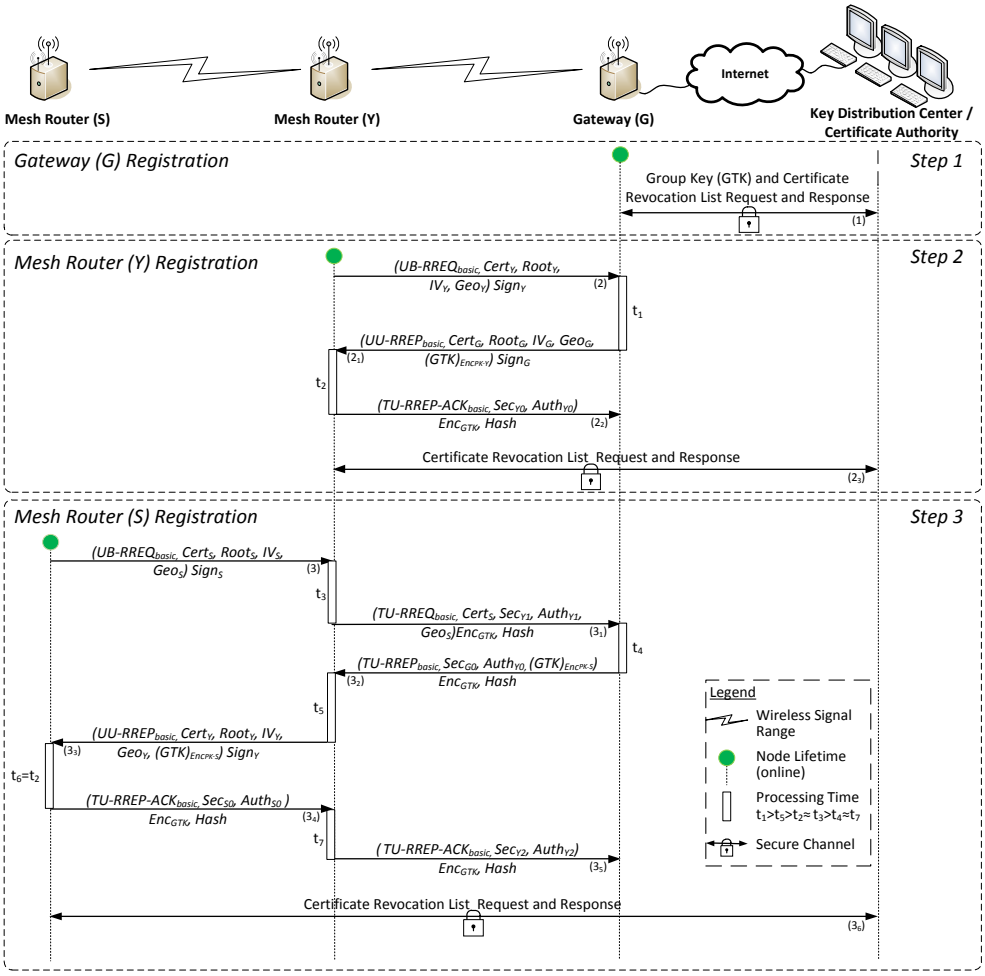

Figure 5. Node Registration Process

E. PASER Operations

In this Subsection, we elaborate all the operations a node undergoes when it executes PASER. These operations are depicted in Figure 4. To ease their understanding, we refer our explanation to a simple example given in Figure 5. The example illustrates three nodes, one gateway (G) and two mesh routers (Y) and (S). These nodes join the network in the order G-Y-S, which corresponds to the depicted steps 1, 2 and 3 respectively.

1) Route Request/Reply/Ack Generation:

- UB-RREQ: This message is generated if and only if a node has no route to the destination. The node creates a UB-RREQ message according to Table II. Hereby, it sets the gateway flag to 1 if the requested destination is a gateway. After creating the message, the node broadcasts it and initializes a RREQ-TIMEOUT timer. Messages (2) and (3) in Figure 5 provide an example of a UB-RREP.
- TU-RREQ: After receiving a UB-RREQ, an intermediate node, that has a route to the destination, generates this message and sends it to the next hop on that route, e.g., message number (3_1) in our example. Hereby, the querying identity remains the UB-RREQ originator identity, whereas *Seq* changes, since the message type has changed.
- UU/TU-RREP: Upon receiving a UB-RREQ or a TU-RREQ, a destination node generates a UU-RREP or a TU-RREP, respectively, e.g., messages (2_1) and (3_2). If the destination is a gateway and the *GFlag* in RREQ is set, the RREP message comprises the group key encrypted with the querying node public key.
- TU-RREQ-ACK: This message is generated by a querying node when it receives a route reply to a query identified by *Seq*. It creates the TU-RREQ-ACK message and sends it to the next hop on its route to the destination, as in messages (2_2) and (3_4).

2) Route Request/Reply/Ack Processing: Based on the querying node Identity and the message sequence parameter *Seq*, a node verifies the freshness of a received message. If it has been previously processed, the message is discarded (replay attack). Otherwise, it extracts the identity of its predecessor and executes the following verifications:

- UB-RREQ/UU-RREP:
  Is the predecessor the owner of the included certificate?
  Is the predecessor in my signal range? Is the difference of our geo-positions smaller than the maximum range of my WLAN device?
  Is the predecessor's message signature valid?
- TU-RREQ/RREP/RREP-ACK
  Is the predecessor a neighbor of mine?
  Is the predecessor's secret fresh?
  Is the predecessor's secret valid?

If one of these verifications fails, the node drops the message (impersonation attack, man-in-the-middle attack, tempering attack or wormhole attack). Otherwise, it updates its tables with the message information. Hereby, it sets the neighbor flag *NeighFlag* of its predecessor to 0 if the received message is a UB-RREQ and the predecessor hasn't been registered yet as a neighbor. Otherwise the *NeighFlag* of the predecessor is set to 1. Depending on the type of the received message, the node afterwards undergoes the following steps:

- UB-RREQ: It checks if it has a route to the destination, if not it updates the message with its own information (e.g., it adds its identity to the route list) and broadcasts it again. Otherwise, it generates a TU-RREQ as described above, e.g., message (3_1).
- TU-RREQ/RREP-ACK: The node updates the message with its own information and forwards it to the next hop on its route to the destination, e.g., message (3_5).
- UU/TU-RREP: It extracts the successor identity and verifies the value of its *NeighFlag*, if it is 0, it forwards a UU-RREP to that node, e.g., message (3_3)and otherwise it forwards a TU-RREP.

3) Route Reply Timeout: This operation occurs at the querying node when the RREQ-TIMEOUT timer expires. The latter happens in either of the following cases: First, no replies from destination, in response to the query, were received or accepted by the querying node, or, second, at least one reply was accepted. In the former case the route discovery is considered failed, while, in the latter case, the route discovery concludes, and the querying node ignores route replies that are further delayed.

Route Discovery Failure: The querying node initiates a new route discovery using a higher value for RREQ-TIMEOUT than the one previously used for the failed route discovery.

Route Discovery Conclusion: Upon accepting a RREP, the querying node considers the discovery concluded after RREQ-TIMEOUT elapses. From all incoming RREP, the querying node always chooses the best route based on the metric field and updates its tables with this route. If the querying node is in the UNREGISTERED state and the discovered route is a route to the gateway, it requests a certificate revocation list via the discovered route, as in messages (2_3) and (3_6). Based on that list, the node verifies if it has fraud routes and deletes them. Afterwards, the node switches to the REGISTERED state.

4) Group Key/Revocation List request: Both requests occur at the end of the node registration phase. It is assumed at this stage of the network setup, that all nodes have a stable route to the CA/KDC. The gateways are anyway provided by a reliable link, e.g., Long Term Evolution (LTE) or satellite, and the mesh routers are typically located during power up near to the fire-fighting command and control vehicle, i.e., they are in the best signal range of the gateways. While the group key request solely occurs at the gateway, message (1), revocation list request occurs at both types of nodes, mesh router and gateway, see messages (1), (2_3) and (3_6). PASER rather specifies the security goals that must be ensured by these requests than the mechanism used. These goals are authenticity and integrity by both requests in addition to confidentiality by the group key request.

V. PASER Analysis

Based on a hop-to-hop trusted relation, PASER promises to achieve the following goals:

Node authentication: This goal is guaranteed by the digital signature in untrusted messages (including revocation list messages) and by the hash tree authentication mechanism in trusted messages - *PASER is robust against impersonation and malign attacks.*

Message freshness and integrity: The freshness goal is provided by the sequence number included in each message. The integrity is achieved by the digital signature in untrusted messages and by the hash element in trusted messages - *PASER is robust against replay and tempering attacks.*

Messages confidentiality: It corresponds to the symmetric encryption of trusted messages, which is mainly applied to combat man-in-the-middle attack. Then, theoretically, an attacker located between two neighbors is able to eavesdrop on trusted messages and prevent the destination from receiving them. As a result, it uses the secrets of these messages to impersonate the messages' sender. Now, due to the encryption in trusted messages, the attacker is not able to reveal those secrets. Apart from that, message confidentiality of trusted messages strongly reduces traffic analysis in PASER. In untrusted messages man-in-the-middle attack is not possible due to the digital signature - *PASER is robust against man-in-the-middle attacks.*

Neighbor transmission authentication: Provided satellite GPS information is not falsified, PASER guarantees to a large extent that node's neighbors are always in that node transmission range. This goal is provided by the fault tolerant distance awareness between new neighbors combined with the achievement of the node authentication goal. - *PASER is robust against wormhole attacks.*

From efficiency perspective, PASER incorporates the following characteristics:

 ISBN: 978-1-61208-010-9

- Nodes always have a route to a gateway.
  - Nodes thereby detect all intermediate nodes on that route.
  - The route is found and maintained in a reactive way. Gateways do not flood the network with beacons.
- It is mainly based on unicast messages, strongly reducing the network overhead of control messages.
- Its security is essentially based on symmetric cryptography, keeping the cost of security mechanisms minimal.

VI. Conclusion and Future Work

In this paper we propose a novel secure and efficient position aware hierarchical route discovery protocol for wireless mesh networks. From a security perspective, the novelty of our approach is its hybrid scheme to secure the route discovery process. This novel combination of digital signature, hash tree authentication scheme and symmetric block cipher yields a huge performance gain while providing a high security level. Another key feature is the integration of nodes' geo-positions in the route discovery, allowing an advanced network management while mitigating a wider range of attacks. Apart from that, dealing with the network as a hierarchical network and building the route discovery process to a large extent upon unicast messages strongly decreases the overhead of this protocol.

In future work we intend to capture explicitly the inherently quantitative nature of security, via a concrete or exact treatment of security using practice-oriented provable security. This enables an exact assessment of how much security the protocol achieves rather than just being secure or non-secure. Furthermore, we designate to thoroughly investigate the performance of PASER in different scenarios experimentally as well as in the simulation to recognize its advantages and its limitations. Apart from that, we intend to analyze the energy consumption imposed by PASER especially by the GPS component it incorporates. Besides, we intend to extend PASER to a route maintenance part and thereby to design an efficient secure routing protocol for wireless mesh networks.

Acknowledgment

Our work has been conducted within the SPIDER project, which is part of the nationwide security research program funded by the German Federal Ministry of Education and Research (BMBF) (13N10238).

References

[1] (2011, May) Security System for Public Institutions in Disastrous Emergency scenaRios (SPIDER). [Online]. Available: http://www.spider-federation.org

[2] A. Wolff, S. Šubik, and C. Wietfeld, "Performance Analysis of Highly Available Ad hoc Surveillance Networks Based on Dropped Units," in *Proc. IEEE International Conference on Technologies for Homeland Security*, Boston, USA, May 2008, pp. 123–128.

[3] (2011, May) Highly Mobile Network Node (HiMoNN). IABG mbH. [Online]. Available: http://himonn.iabg.de/index.php?lang=en

[4] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) routing," RFC 3561, Jul. 2003.

[5] I. Chakeres and C. Perkins, "Dynamic MANET On-Demand (DYMO) Routing," draft-ietf-manet-dymo-21, Jul. 2010.

[6] T. Clausen and P. Jacquet, "Optimized Link State Routing (OLSR) Protocol," RFC 3626, Oct. 2003.

[7] K. Sanzgiri, D. Laflamme, B. Dahill, B. N. Levine, C. Shields, and E. Belding-Royer, "Authenticated Routing for Ad hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 598–610, Mar. 2005.

[8] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," *ACM Journal on Wireless Networks*, vol. 11, no. 1-2, pp. 21–38, Jan. 2005.

[9] L. Buttyán and I. Vajda, "Towards Provable Security for Ad hoc Routing Protocols," in *Proc. 2nd ACM Workshop on Security of Ad hoc and Sensor Networks (SASN)*, Washington DC, USA, Oct. 2004, pp. 94–105.

[10] M. Burmester and B. de Medeiros, "On the Security of Route Discovery in MANET," *IEEE Transactions on Mobile Computing*, vol. 8, no. 9, pp. 1180–1188, Feb. 2009.

[11] L. Abusalah, A. Khokhar, and M. Guizani, "A Survey of Secure Mobile Ad hoc Routing Protocols," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 4, pp. 78–93, 2008.

[12] *IEEE P802.11s*, IEEE Draft Amendment: Mesh Networking, Rev. 10.0, Mar. 2011.

[13] (2011, May) Better Approach To Mobile Ad hoc Networking (B.A.T.M.A.N.). Freifunk Community. [Online]. Available: http://www.open-mesh.org/

[14] *Digital Signature Standard (DSS)*, National Institute of Standards and Technology (NIST) Std. FIPS PUB 186-3, Jun. 2009.

[15] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," in *Proc. 9th Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2007*, ser. Lecture Notes in Computer Science (LNCS), no. 4727. Springer-Verlag, 2007, pp. 450–466.

[16] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996, ch. 13, p. 556.

[17] (2011, May) Cryptographic Hash Algorithm Competition. National Institute of Standards and Technology (NIST). [Online]. Available: http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

[18] T. Tran, M. Sbeiti, and C. Wietfeld, "A novel Role- and Certificate-based Single Sign-On System for Emergency Rescue Operations," in *IEEE International Conference on Communications - ICC*, Jun. 2011, pp. 1–6.

 ISBN: 978-1-61208-010-9