24

Security of Access in Hostile Environments Based on the History of Nodes in Ad Hoc Networks

Saud Rugeish Alotaibi
De Montfort University
United Kingdom, England

1. Introduction

An ad hoc wireless network is built on cooperation between two or more nodes with wireless links and networking capability. The major applications of such networks today are tactical military and other security-sensitive operations. For example, military and police units (e.g. soldiers, tanks, police cars) equipped with wireless communication devices can form ad hoc wireless networks when they roam in insecure environments. Such networks can also be used for emergency, law enforcement and rescue missions. Since they have relatively low cost and can be deployed rapidly, they also constitute a viable option for commercial uses such as sensor networks and emergency situations, and there is a trend to adopt them for commercial uses due to their unique properties. The most critical challenge in the design of these networks is their security in hostile environments [81-86].

Their nodes are independent units which rely not on a central infrastructure but on neighbouring nodes to route each packet to the destination node. Ad hoc wireless networks can therefore work properly only if the participating nodes cooperate with each other in routing and forwarding. Nodes lack physical protection and are always under threat of being captured and compromised. They carry user and device histories, as each node can obtain data on all events involving a specific user and a specific device; therefore, each has to be able to document the user and the device at the registration stage.

The security requirements for different services range from highly security-sensitive military tactical operations, such as battlefields, rescue missions and emergency situations, to instantaneous classroom applications and areas where density is too small to justify economically the deployment of a network infrastructure. Attacks on ad hoc wireless networks can come from any direction and can target any node. Thus, ensuring a secure environment is as important as for wired networks, which have several lines of defence such as firewalls and gateways. Security depends on access to the history of each unit, which is used to calculate the cooperative values of each node in the environment. The calculated cooperative values are then used by the relationship estimator to determine the status of the nodes. Every node should be capable of making its own security decisions based on cooperation with other peer nodes.

The rest of the chapter is organized in the following manner. Section 2 discusses the requirements for any security solution, while section 3 explains the secure environment.

Section 4 describes the creation of public/ private keys and digital certificates, section 5 sets out the components of our architecture, section 6 presents and explains the activity diagram and section 7 presents a case study. Section 8 concludes the chapter.

2. Security requirements

The following are the security requirements to be met by a secure environment:

- **Authentication**: Ensures the identity of the node with which the communication is carried out. This avoids impersonation.
- **Availability**: Ensures that the eligible nodes are able to obtain the required services despite denial-of-service attacks.
- **Non-repudiation**: Ensures that a node cannot deny a particular action performed by it at a later stage. This could help in the detection of compromised nodes.
- **Detection of malicious nodes**: Ensures that nodes are capable of detecting the presence of malicious nodes in the environment, thus avoiding the participation of such nodes in the routing process.
- **Stability**: Ensures that a node is able to revert to its normal operating state within a finite time after any attack.

3. Secure environments

In a secure environment, some of the ad hoc nodes are involved in other infrastructure-based wireless networks such as WLANs and cellular systems; therefore, each of the ad hoc nodes will belong to an operation service provider (OSP), as shown in Figure 1. Other non-managed ad hoc network nodes, which are not involved in any other wireless networks, will be managed by the OSP, in order for those undefined nodes or networks to be able to access our secure environment. The following sections show how our SE consists of a number of ad hoc wireless networks interconnecting with each other.

3.1 Node classification

Nodes in the SE are classified thus:

- **User Nodes** are normal ground nodes; typically, soldiers equipped with devices of limited communication and computation ability whose duty it is to collect data and transfer it to a network backbone node.
- **Network Backbone Nodes** are usually units or master nodes located within the same network, for example in towers or tanks. NBBNs can establish direct wireless links to communicate amongst themselves.
- **Operation Service Providers** are usually units in the environment. This type of node will have many management, registration and control functions, such as duty signing and creating new certificates for different nodes in the secure environment.

3.2 Node documentation

All nodes in the secure environment are also placed into three categories according to their documentation status.

- **Documented nodes** are those which are documented by the OSP. Information on these nodes and their history is stored in a database (DB) authenticated by the OSP.

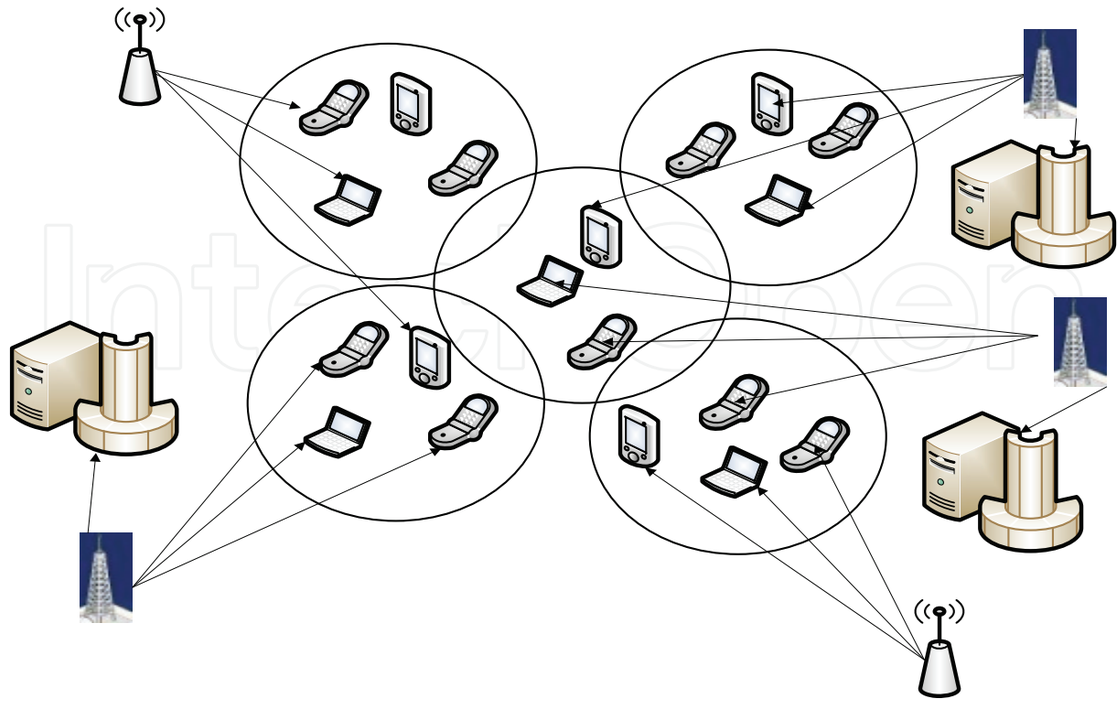


Fig. 1. Secure environment

- **Certificate-documented nodes** are those which possess a certificate issued by the OSP. They will have come into contact with a secure environment earlier and the certificate will verify that they are secure. Information on these nodes is stored in the documented DB of the OSP and they do not have any history in the documented DB.
- **Undocumented nodes** are those in the secure environment which do not fall into either of the above two categories. This category may also contain nodes which could have been certificate-documented by an OSP, but remain undocumented because there has been no need to verify their certificates.

4. Digital operation certificate management framework

This section describes the certificate management system of a secure environment. It shows how public/private keys and digital operation certificates are created. It also illustrates the process of certificate revocation.

4.1 Creation of public/ private keys and digital certificates

The public keys and the corresponding private keys of secure environment nodes are created by the OSP, which also issues the public-key certificates of SE nodes. Since a key is unique, (K_{public}) is unique and thus $H(K_{public})$, the fingerprint of K_{public}, is also unique and is considered the identifier in an SE. The operation certificate is used as permission to access this environment. Each node in the secure environment holds its digital operation certificate in its node database. The main structure of digital operation certificates contains [70] the MAC address of the node, its public key, the name of the OSP issuing this certificate, the certificate issue and expiry dates and the public key of the OSP. Finally, the contents of the certificate are attached to the digital signature of the OSP.

- **Node Identifier (ID)**: Holder of the certificate
- **MAC address of device (Mac)**: The unique serial number of the device
- **Node Public Key (K_{public})**: A unique key that is the fingerprint of the user
- **Certificate Operation OSP Identifier**: Name of the OSP that created and signed the certificate
- **Certificate Issue Date/Time**: The first day on which the certificate is valid
- **Certificate Expiry Date/Time**: The last day on which the certificate is valid
- **OSP Digital Signature**: Digital signature of the OSP.

4.2 Digital operation certificate distribution

Certificate distribution is a very important and low-cost mechanism that allows SE nodes to send the certificates they hold. Each node periodically starts receiving its physical neighbour (in one hop), its digital operation certificate and the corresponding OSP's public key stored in its NDB. Each node receives these certificates, compares them with its NDB and adds whatever new certificates it does not hold, as well as the public keys of its issuer; or it adds the renewal of an expired, extant certificate. The certificate distribution process is repeated at regular time intervals (RTIs). All nodes will have almost all digital operation certificates based on the mobility of the nodes and the RTI.

4.3 Revocation of digital operation certificates

The digital certificate management system provides certificate revocation as one of its basic services. There are two types of certificate revocation in our algorithm. Explicit revocation occurs when any node has a certificate and the OSP revokes it. The OSP sends the corresponding revocation to the other nodes belonging to the SE. If it cannot send the corresponding revocation for any reason, the renewal of the certificate can be denied, resulting in an implicit revocation.

In general, the OSP, when issuing the certificate, determines its issuing and validity times. All certificates are revoked after their expiration time. Therefore, the OSP should be updated about the certificates of SE nodes before the expiration time. In both types of revocation, when the OSP provides the SE nodes with information about any certificate, it should be distributed through the exchange process. In this way the nodes in the secure environment will be provided with this new information. Consequently, the OSP is responsible for the certificate revocation process and for transferring these revocations to all SE nodes. All SE nodes are informed when any of them carries out an explicit revocation and their NDBs are subsequently modified. This revocation will be distributed to the other nodes in the secure environment, both by certificate distribution and the process by which NDBs are merged.

The OSP is responsible for updating those certificates that have been implicitly revoked at regular intervals. Each SE node that has a new certificate will update its NDB, and then transfer the new certificate to its neighbours through the certificate distribution process. If any node does not receive the new certificate through the distribution and merging processes, and needs to validate the key, a new certificate will be requested from the OSP itself.

5. Components of our architecture

The components of our architecture are as follows:

User Nodes, as set out in 3.1 above, are typically soldiers or persons equipped with devices of limited communication and computation ability, whose duty is to deal with nodes, collect data and transfer them to NBBNs.

Network Backbone Nodes are usually units or master nodes located within the same network, for example towers or tanks. NBBNs can establish direct wireless links for communication among themselves. There are three divisions which carry out many functions (management, observation, control and so on) for the network. Their responsibility is to collect data, to observe nodes entering the network and to record the histories and certificates of all other nodes.

Operation Service Providers are usually units in the environment whose five divisions carry out many functions (management, registration, control and so on) for that environment. Their responsibility is to register new nodes, collect and analyse data, update the history of nodes and observe nodes entering the environment. The OSP has six units, which are the Registration Unit (RU), the Operation Certificate Unit (OCU), the Data Packet Collection Unit, the Analyser Unit (AU), the History Model Unit and the Database Unit.

The responsibility of the **Registration Unit** is to register a new node and apply the policy of the unit. Registration is an important stage before issuing a digital operation certificate for a node, as it verifies the identity of the user. This is the function of the RU. The user provides the RU with essential information: the user's name, the MAC address of the device and the fingerprint of the user.

The **Operation Certificate Unit** is the main service provided by the OSP. When the OCU receives a certification request from the RU, the OSP issues a digital operation certificate and signs it with its private key. The structure of the certificate should be defined by being standardised to ITU-T recommendation X.509, for example. All the information needed to complete the certificate will be provided by the RU.

The **Data Packet Collection Unit** collects the data packets in a secure environment and saves them in the main buffer. The data collector enables the packet analyser to use data collection containers to analyse all available data that the system has collected from the different nodes. At the same time it enables the packet analyser to process the transferred information, which can be used to obtain and save data that is gathered from several sources [106].

The **Database Unit** stores information on each node in a secure environment, including information regarding the history model of each node. It also keeps information like H (K_{public}), K_{public}, the fingerprints of each node and the MAC address of each device. Finally, it holds information regarding digital operation certificates and their revocation, to help in restricting future access with the same certificate.

The **History Model Unit** is used to calculate the cooperation values of each node in the environment. Our secure environment access system uses the history of nodes to build several lines of protection, equivalent to firewalls and gateways in wired networks. This unit receives data on the classification of nodes from the analyser base to analyse the packets. There are three kinds of node, as follows.

1. Positive Node (POSN). This is considered a cooperative node which, concerning packets or messages, will:
   - Notify its neighbours of any misbehaviour
   - Send an update to its neighbours when it receives new information
   - Forward any notification it receives from the OSP or NBBN
   - Notify its neighbours about any problem occurring with itself.

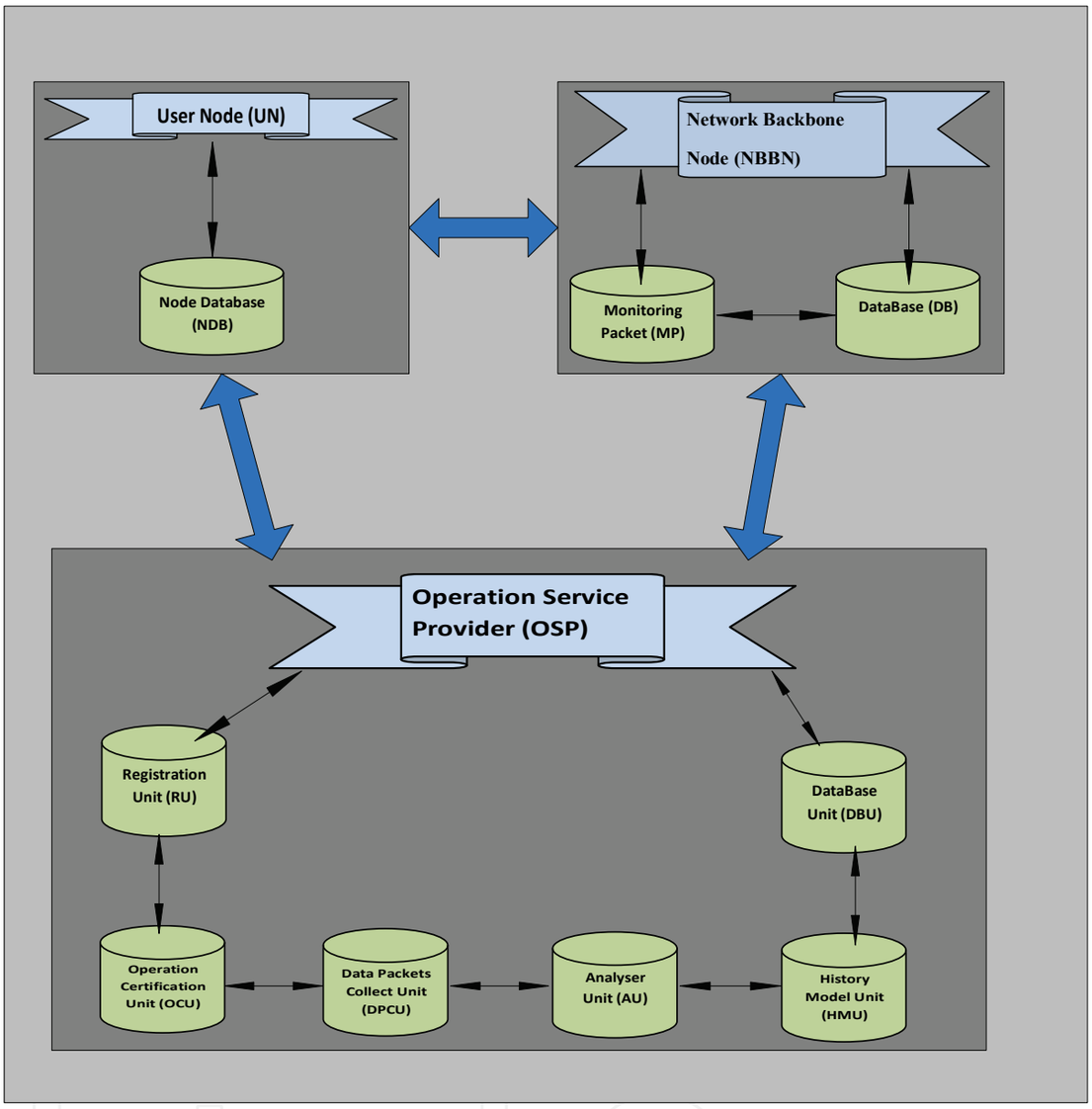


Fig. 2. Components of our architecture

The history of positive node

$$(\text{HPOSN}) = \frac{\Sigma \text{ all events of (POSN)}}{\Sigma \text{ all events of node}} \quad (1)$$

2. Natural Node (NATN). This is considered an uncooperative node and carries out normal work, such as:
   - Regular forwarding
   - Sending regular updates to its neighbours
   - Sending acknowledgment messages

The history of natural node

$$(\text{HNATN}) = \frac{\Sigma \text{ all events of (NATA)}}{\Sigma \text{ all events of node}} . \quad (2)$$

3. Negative Node (NEGN). This type misbehaves and does not send natural packets and messages. It is not considered a natural node because it:
   - Does not perform regular forwarding
   - Does not send regular updates to its neighbours
   - Does not send acknowledgment messages
   - Carries out misbehaviour
   - Tries to attack, for example by sending invalid certificates or invalid public keys, or sending many packets to a specific node.

The history of negative node

$$\left(\text{HNEGN}\right) = \frac{\Sigma \text{ all events of (NEGN)}}{\Sigma \text{ all events of node}} \quad (3)$$

The **Analyser Unit** checks each packet or message in the secure environment that the main buffer has collected. It then classifies all packets according to their contents. The analyser deals with all definition of packets and messages. It has the ability to define and classify unknown packets and add to the classification. The analyser will classify the nodes in the secure environment into three categories, POSN, NATN and NEGN, according to Table 1.

Event and behaviour	Positive Node	Natural Node	Negative Node
Regular forwarding		√	
Sends regular updates to its neighbours		√	
Sends acknowledgment messages		√	
Notifies its neighbours of any misbehaviour by others	√		
Send updates to its neighbours when it receives new information	√		
Forwards any notification it has received from OSP or NBBN	√		
Notifies its neighbours of any problem occurring with itself	√		
Carries out misbehaviour			√
Tries to attack (sends invalid certificate or invalid public key, or sends many packets to a specific node)			√

Table. 1. Node classification by analyser unit

6. Activity diagram

The activity diagram (Figure 3) depicts the steps taken by a node while handling requests to access a secure environment. The following are the steps shown in the activity diagram:

- Request from node *J* to node *I*
- Node *I* checks whether node *J* is registered
- If node *J* is not registered and node *I* ignores its request then node *J* transfers to the registration stage.

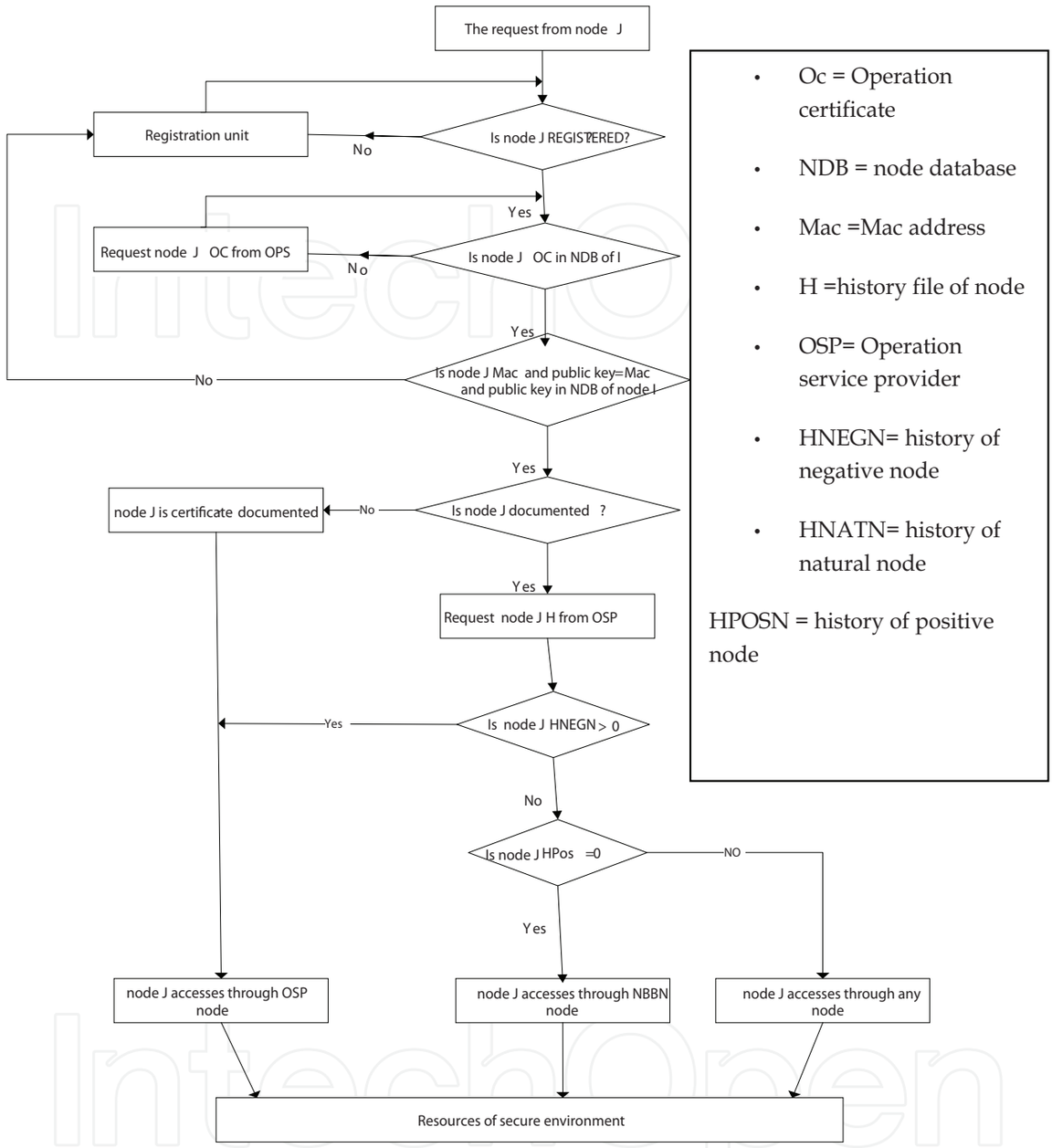


Fig. 3. Activity diagram

- If node *J* is registered then node *I* checks for the operation certificate (OC) of node *J* in its database.
- If the OC of node *J* is not in the database then node *I* requests it from the OSP.
- If the OC of node *J* is in the database then node *I* checks that the MAC address and public key of node *J* are valid
- If the MAC address and public key of node *J* are not valid then node *I* ignores its request and node *J* transfers to the registration stage
- If the MAC address and public key of node *J* are valid then Node *I* checks whether node *J* is documented

- If node *J* is not documented, then it is certificated-documented
- If node *J* is certificated-documented then it can access the secure environment through the OSP
- If node *J* is documented then node *I* requests the history of node *J* from the OSP.
- If the history of negative node of node $J > 0$ then Node *J* can access the secure environment through the OSP
- If the HNEGN of node $J < 0$ then If the HPOSN of node $J = 0$ then Node *J* can access the secure environment through an NBBN.
- ELSE node *J* can access the secure environment through any node.

7. Formal description

The formal description of the Secure Environment (SE) is as follows.

7.1 Network model

In a secure environment, some of the ad hoc nodes are involved in other infrastructure-based wireless networks such as WLANs and cellular systems; therefore, each of the ad hoc nodes will belong to an operation service provider (OSP), as shown in Figure 1. Other non-managed ad hoc network nodes, which are not involved in any other wireless networks, will be managed by the OSP, in order for those undefined nodes or networks to be able to access our secure environment. Our secure involves a number of MANET interconnecting with each other; in addition all PKI are pre-connected by wireless connection to exchange data, and to update information.

Pki: Public key of network *i*, $1 \le i \le n$;

Those OSP are fully trusted by all nodes that belong to this secure environment. Nodes in the SE are classified thus:

- User Nodes(UN) are normal ground nodes;
  n: Number of networks in the SE; networks are numbered from 1 to *n*;
- Network Backbone Nodes(NBBN) are usually units or master nodes located within the same network,
  ni: Number of nodes, including Network Back Bone Node (NBBN), in the network *i*, $1 \le i \le n$; nodes in a network *i* are numbered from 1 to *ni*;
- Operation Service Providers (OSP) is usually units in the environment.
  k*i*: Number of Operation Service Providers (OSPs) in SE *i*, $1 \le \ \le n$;
  Pki: Public key of network *i*, $1 \le i \le n$;

7.2 Behaviour model

In a secure environment, the behaviour of nodes capture by operating service node (OSP) and stores in history file of behaviours that nodes might have (positive node , negative node and natural node). Positive Node (POSN) This is considered a cooperative node which, concerning packets or messages, will: Notify its neighbours of any misbehaviour, Send an update to its neighbours when it receives new information, Forward any notification it receives from the OSP or NBBN and Notify its neighbours about any problem occurring with itself.

POSN: Positive node in the SE, for $1 \le i \le n$.

Natural Node (NATN), this is considered an uncooperative node and carries out normal work, such as: Regular forwarding, Sending regular updates to its neighbours and sending acknowledgment messages.
NATN: Natural node in the SE, for $1 \leq i \leq n$.
Negative Node (NEGN), this type misbehaves and does not send natural packets and messages. It is not considered a natural node because it: Does not perform regular forwarding, does not send regular updates to its neighbours, does not send acknowledgment messages, carries out misbehaviour, tries to attack, for example by sending invalid certificates or invalid public keys, or sending many packets to a specific node.
NEGN: Negative node in the SE, for $1 \leq i \leq n$.
During specific period of time; this capture is always updated depending on the observed node actions, despite the fact that saving all behaviours is impossible; nevertheless, a reasonable number of behaviours must be stored.

7.3 Mobility model

Our secure environment (SC) is proposed for *ad hoc* wireless networks with a minimum number of mobile nodes. The proposed algorithm requires a different minimum number of nodes in the network to guarantee establishment of connection between nodes. In secure environment (SC), each node sends an RREQ packet to only one neighbor or operating service provider (OSP). In an ad hoc network, however, there are many situations where mobile nodes move together or form groups (the heading direction angle of nodes in each group is nearly similar). For example, vehicles on a road or, in a military scenario, a group of soldiers searching a particular plot of land, all working together in a cooperative manner to accomplish a common goal.
The following variables represent the parameters of the SE:

- n: Number of networks in the SE; networks are numbered from 1 to n;
- ni: Number of nodes, including Network Back Bone Node (NBBN), in the network i, $1 \leq i \leq n$; nodes in a network i are numbered from 1 to ni;
- ki : Number of Operation Service Providers (OSPs) in SE i , $1 \leq i \leq n$;
- h_i : History of node in SE i , $1 \leq i \leq n$;
- DOCxj: Digital Operation Certificate of node i in the SE, for $1 \leq i \leq n$
- DOCM : Documented of node i in the SE, for $1 \leq i \leq n$
- C-DOCM: Certificate -Documented of node i in the SE, for $1 \leq i \leq n$
- 2POSN: Positive node i in the SE, for $1 \leq i \leq n$
- NATN: Natural node i in the SE, for $1 \leq i \leq n$
- NEGN: Negative node i in the SE, for $1 \leq i \leq n$
- HPOSN: History of positive node i in the SE, for $1 \leq i \leq n$
- HNATN: History of natural node i in the SE, for $1 \leq i \leq n$
- HNEGN : History of negative node i in the SE, for $1 \leq i \leq n$
- *Pubij*: Public key of the node j in the network i , for $1\ j \leq ni$ and $1 \leq i \leq n$;
- *Prvij*: Private key of the node j in the network i , for $1\ j \leq ni$ and $1 \leq i \leq n$;
- *Pki* : Public key of network i , $1 \leq i \leq n$;
- MAC i : MAC address of node i , $1 \leq i \leq n$

Before defining our access mechanism, healthiness conditions for the above variables must be defined.

- $Pkij \neq Pkuv$ for $i \neq u$ or $j \neq v$
- $Pubi \neq Pubj$ for $i \neq j$
- $Prvi \neq Prvj$ for $i \neq j$
- $MAC\ i \neq MACj$ for $i \neq j$

After showing the healthiness of our variables, our access mechanism can be described by the following steps, where Ti denotes the i^{th} component of a tuple T:

1. Granting certificate and history authority duties to nodes:
   - $\forall i,j.\ 1 \leq j \leq ni \wedge 1 \leq i \leq n \wedge OSP\ ij=ti.$ (1)
2. Issuing digital operation certificates to local nodes of each network:
   - $\forall i,j.\ 1 \leq j \leq ni \wedge 1 \leq i \leq n \wedge DOCdij = <j, i, sdxij, edxij, OSPi, Pkij, MACij, CALij \ldots, Sign\ xij>$ (2)

   Where $OSPi$ is the OSP of the node j in the network i; $sdxij$ and $edxij$ are the start and end date of the digital operation certificate; and the digital signature of the certificates $Sign\ xij$ is calculated by the $OSPi$ of the network i by performing threshold cryptography. $CALij$ is the type of node based on the registration.
3. Recording history certificate to local nodes of each network:
   - $\forall i,j.\ 1 \leq j \leq ni \wedge 1 \leq i \leq n \wedge Hxij = <j, i, shxij, uhxij,$ OSP$i, Pkij, HPOSNij, HNATNij, HNEGNij, \ldots \ldots, CLLAij, Signxij>$ (3)

   Where OSPi is the OSP of the node j in the network i; $shxij$ and $uhxij$ are the start and update of the history file; $HPOSNij$, $HNATNij$ and $HNEGNij$ are the history file of the node and the OSP of the network i calculated from their events. $CLLA\ ij$ is the kind of node that it will be after calculation.

   Each node uses its digital operation certificate and history certificate in order to access services in the SE through another node. A node needs to request from its OSP a new history certificate and operation certificate in order to perform in it.
4. A request for digital certificates from a node j of the network t to another node can be modelled by a message of the form:

$$\langle \boldsymbol{j, i, W, Z} \rangle \tag{4}$$

   for some digital operation certificate W and some history certificate Z.

   Such a request $\langle j, i, W, Z \rangle$ is checked as follows:

   a. The requester is the owner of the digital operation and history certificates, i.e.

$$(\boldsymbol{W^1} = \boldsymbol{j}) \wedge (\boldsymbol{Z^1} = \boldsymbol{j});$$

   b. The OSP is the node where W and Z were issued, i.e.

$$(\boldsymbol{W^2} = \boldsymbol{i}) \wedge (\boldsymbol{Z^2} = \boldsymbol{i});$$

   c. These certificates have not expired, i.e.

$$(\boldsymbol{W^3} \leq CD \leq \boldsymbol{W^4}) \wedge (\boldsymbol{Z^3} \leq CD \leq \boldsymbol{Z^4});$$

   Where CD denotes the current date;

   d. Certificates W and Z are authenticated using the public key Pk_i of the network t and a signature verification algorithm for threshold cryptography.

5. The requester node can access services in SE as follows:
   a. It has access through the OSP when the its history certificate is negative
      - *Hxij*=<*j*, *i*, *s*h*xij*, uh*xij*, *OSPi*, *Pkij*, *HPOSNij*, *HNATNij*, *HNEGNij*……. *HNEGNij*, *Signxij*> (9)

$$Node(i)access \rightarrow OSP\ if\ H(i) = negative$$

   b. It has access through NBBN when its history certificate is natural
      - *Hxij*=<*j*, *i*, *s*h*xij*, uh*xij*, *OSPi*, *Pkij*, *HPOSNij*, *HNATNij*, *HNEGNij*……. *HNATNij*, *Signxij*> (10)

$$Node(i)access \rightarrow NBBN\ if\ H(i) = natural$$

   c. It has access through any anther node when the its history certificate is positive
      - *Hxij*=<*j*, *i*, *s*h*xij*, uh*xij*, *OSPi*, *Pkij*, *HPOSNij*, *HNATNij*, *HNEGNij*……. *HPOSNij*, *Signxij*> (11)

$$Node(i)access \rightarrow Node(j)\ if\ H(i) = postive$$

8. Case study

Wireless *ad hoc* networks of networks (WANETs) are considered to be the future of wireless networks owing to their specific characteristics: practicality, simplicity, self-organization, self-configuration, ease of use and low cost when operating in a licence-free frequency band. There are many applications of *ad hoc* networks, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic ones such as:

- In education, for students to interact with teachers during classes via laptops
- Healthcare and telecare systems
- Inter-vehicle communications; for example, sending instant traffic reports and other information between drivers
- Email and electronic file transfer
- Web services that can be used by *ad hoc* network users where a node in the network serves as a gateway to the outside world
- A wide range of military applications, such as a battlefield in unknown territory where an infrastructure network is not available or impossible to maintain
- Collaborative work for business environments
- Emergency search-and-rescue operations in disaster areas, where it is almost impossible to implement an infrastructure network
- Personal area networking and Bluetooth
- Electronic payments from anywhere (i.e. taxi)
- Home wireless networks and smart homes
- Office wireless networks.

In this section, we evaluate our secure environment system, concentrating on access to the SE. A military case study with two scenarios will be introduced. The first highlights our secure environment system, concentrating on our access control prevention technique for predefined armies in an unknown and unstable military environment; this scenario combines authentication, authorisation, confidentiality and integrity to provide privacy

protection for elements and tactics. The second scenario illustrates an SE system in an unstable and unknown military environment, showing event detection techniques combined with policies to provide a secure military system against unknown elements.

8.1 Military environment

This military case study considers a battlefield in unknown territory, where infrastructure deployment is hard to achieve or maintain; therefore, SE will be the perfect solution. The military domain is a very challenging environment characterised by ambiguity and the need to be able to deal with significant and disruptive dynamic changes. The goals of military systems are mainly concerned with the ability to provide a secure environment for their components, because opponents (enemies) are always trying their best to break down or destroy our activities. Therefore, our secure environment concentrates on prevention and detection mechanisms.

8.2 Definition of components

In the military environment, a critical system and the specification of the security requirements for its components are essential. Registration, authentication and authorisation are among the most important requirements, but before defining and analysing them, we need to define our military system and its elements. We will be dealing with a military alliance consisting of different armies (e.g. NATO); each army will be defined as a WANET, while the whole alliance is defined as an SE. Each of the armies comprises different elements, from a soldier to the commander-in-chief. Usually in the military, there will be a specific hierarchy, in which each officer will have the authority to give orders or to communicate with different elements based on his/her rank.

- Each army is classified as a WANET
- WANETs merge to create a military alliance which is an SE
- NATO is defined as the OSP for all armies
- Soldiers in our SE will be defined as normal *ad hoc* nodes (negative, positive and nautral)
- Base stations, tanks, trucks and military aircraft are defined as NBBNs
- A set of policies is defined for each WANET (army).

8.3 Securing the military environment

Our military alliance will be a merger of different WANETs creating the SE, depicted in Figure 4.

The first step in providing a secure military system is to set up an operational process for the SE components; this is done by distributing operation certificates, which are initially granted by the SE. These certificates act as identity documents for each element of the military SE. As with the operation certificates, each OSP distribute certificates to enable specific nodes to carry out leading and agile operations.

Two scenarios are now considered for the military environment.

8.4 Scenario one

The first scenario assumes a military alliance of two armies (B and F), each of which has all kind of nodes (positive, negative and neutral). Before defining the SE to provide authorisation and authentication to other nodes, a few points must be clarified in our scenario:

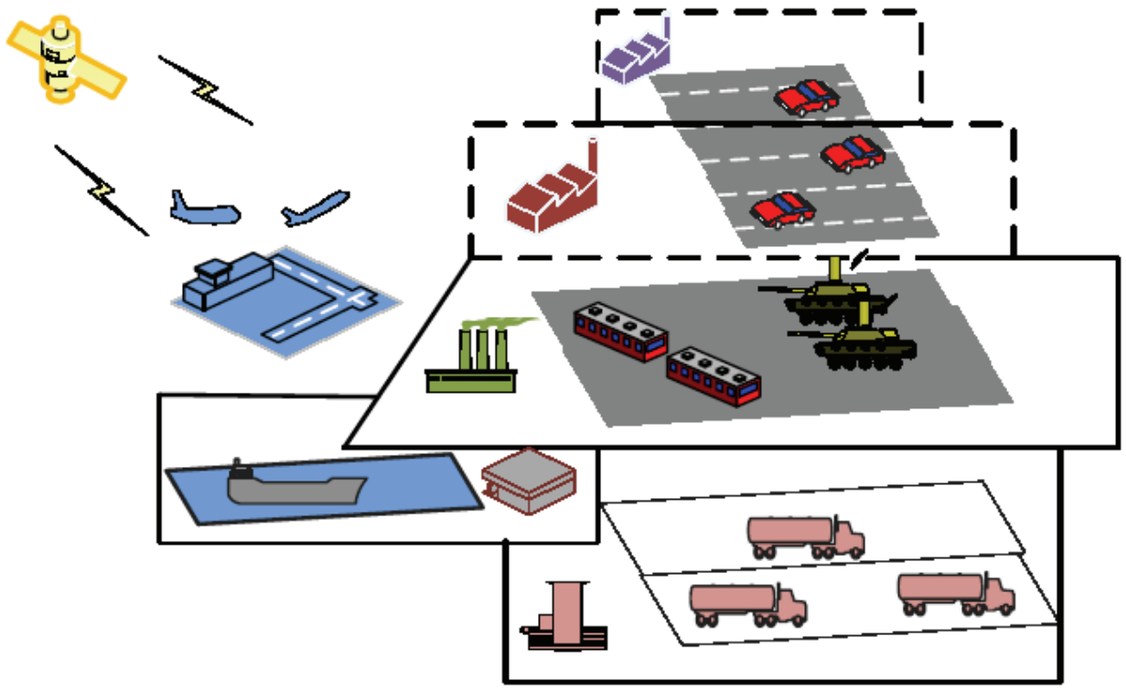


Fig. 4. Secure environment community

- Armies can join and disconnect without affecting the SE system.
- The public keys of the digital operation certificate are known between all elements in the whole SE.
- All nodes (soldiers) have received their operation certificates from their OSPs.
- The OSPs have sent the history of the nodes to the NBBNs.
- Each WANET has a set of policies.
- All nodes in the SE must be registered at the registration stage.

To provide a secure environment in this scenario, the first step is to ensure administration; as previously mentioned, the OSP and the NBBNs will carry out the administration. Their duties are to guarantee that elements from different armies can communicate and engage with different elements in the SE system and to provide all nodes with updates on the history of other nodes.

The second step is to provide or prevent access to the most essential components, which are needed in any community. Such prevention and access are needed for the authentication (by operation certificate) and authorisation (by node history status) of the SE elements. For instance, if a node (soldier) from the British army is trying to connect through the French army, this node will be authenticated (verified) by the NBBN of the French army by his operation certificate. Meanwhile, the granting of history status will be based on the policies (positive, negative and natural) of the node to access the SE through the French army.

The third step is the containment and recovery component. When a problem has occurred during any military operation, specific rules and procedures usually apply; for example, if members of a F platoon have been captured, the enemy will try its best to extract the private key in order to gain access to all secret information and to forge new certificates in order to break the system down. In this situation, the OSP of the SE will try to regenerate new shares of the private key, to make sure that it is kept safe during military operations. Moreover, the

history file of this node, updated via links through heterogeneous cards available with NBBNs (e.g. satellites and cellular), will be used to receive orders from the main station OSP of the SE to which the NBBN belongs.
To elaborate on our secure system and to show the components providing authentication and authorisation between the military elements in the SE, the following specification formalism will be introduced:

Xij: soldiers *i* from army *j*; $i \geq 1$; *j* = NATO countries;
Yij: tanks, trucks and military aircraft *i* from army *j*; $i \geq 1$; *j* = NATO countries;
Zi: base station and cellular (OSP) *i* from SE; $i \geq 1$.
DOCM: Documented node i in the SE, for $1 \leq i \leq n$
POSN: Positive node i in the SE, for $1 \leq i \leq n$
NATN: Natural node i in the SE, for $1 \leq i \leq n$
NEGN: Negative node i in the SE, for $1 \leq i \leq n$
HPOSN: History of positive node i in the SE, for $1 \leq i \leq n$
HNATN: History of natural node i in the SE, for $1 \leq i \leq n$
HNEGN: History of negative node i in the SE, for $1 \leq i \leq n$
Hi: History certificate of node in SE i, $1 \leq i \leq n$;
DOCxj: Digital Operation Certificate of node i in the SE, for $1 \leq i \leq n$
Pki: public key of network i, $1 \leq i \leq n$;
MAC i : MAC Address of node i, $1 \leq i \leq n$

8.4.1 Authentication and authorisation between elements of an army in the SE military system

- Authentication (*X1* B, *X2* B) between soldiers in the same army is based on the *X* operation certificate, where *X* is received from base station *Z*. The certificate will be verified using the B public key and the MAC address of *X*.

$$DOCxij =< j, i, sdxij, edxij, OSPi, Pkij, MACij, CALij..., Signxij >$$

$$X(B1 \vee B2) \Rightarrow \begin{cases} drop(req) & if \;\; DOC(X(B1 \vee B2)) \neq valid \\ Accept(req) & if \;\; DOC(X(B1 \vee B2)) = valid \end{cases}$$

- Authorisation (*X1* B, *X2* B) between soldiers in the same army is based on the history file of *X* and its status, where *X* is received from base station *Z* or *Y* and will be granted only for positive *X*.

$$Hxij =< j, i, \text{sh}xij, \text{uh}xij, OSPi, Pkij, HPOSNij, HNATNij, HNEGNij...CLLAij, Signxij >$$

$$X(B1 \vee B2) \Rightarrow \begin{cases} drop(req) & if \quad H(B1 \vee B2) \neq positive \\ Accept(req) \wedge access \rightarrow X \; if \; HB(1 \vee 2) = positive \end{cases}$$

- Authentication (*Y1* B, *Y2* B) between tanks or trucks in the same army is based on the *Y* operation certificate, where *Y* is received from the base station *Z*. The certificate will be verified using the B public key and MAC address of *Y*.

$$DOCxij =< j,i,sdxij,edxij,OSPi,Pkij,MACij,CALij...,Signxij >$$

$$YB(1 \vee 2) \Rightarrow \begin{cases} drop(req) & if \quad DOC(YB(1 \vee 2)) \neq valid \\ Accept(req) & if \quad DOC(YB(1 \vee 2)) = valid \end{cases}$$

- Authorisation (*Y1* B, *Y2* B) between tanks or trucks in the same army is based on the history file of *Y* and its status, where *Y* is received from base station *Z* and will be granted only to positive and natural *Y*.

$$\mathrm{H}xij = j,i,\mathrm{sh}xij,\mathrm{uh}xij,OSPi,Pkij,HPOSNij,HNATNij,HNEGNij...CLLAij,Signxij >$$

$$YB(1 \vee 2) \Rightarrow \begin{cases} drop(req) & if \quad H(1 \vee 2) = negative \\ Accept(req\ ) \wedge access \rightarrow Y & if\ H(1 \vee 2) \neq negative \end{cases}$$

- Authentication (*Y1* B, *X2* B) between tanks or trucks and soldiers from the same army is based on *Y* and *X* operation certificates, where *Y* and *X* are received from base station *Z*. The certificates will be verified using the B public key and MAC addresses of *Y* and *X*.

$$DOCxij =< j,i,sdxij,edxij,OSPi,Pkij,MACij,CALij...,Sign\ xij$$

$$XB \vee YB \Rightarrow \begin{cases} drop(req) & if \quad DOC(X \vee Y) \neq valid \\ Accept(req) & if \quad DOC(X \vee Y) = valid \end{cases}$$

- Authorisation (*Y1* B, *X2* B) between tanks or trucks and soldiers in the same army is based on the history files of *Y* and *X* and their status, where *Y* is received from base station *Z*, and will be granted only to positive and natural *Y*s or *X*s.

$$\mathrm{H}xij =< j,i,\mathrm{sh}xij,\mathrm{uh}xij,OSPi,Pkij,HPOSNij,HNATNij,HNGENij...CLLAij,Signxij$$

$$XB \vee YB \Rightarrow \begin{cases} drop(req) & if \quad H(X \vee Y) \equiv negative \\ Accept(req) \wedge access \rightarrow X \vee Y & if \quad H(X \vee Y) \neq negative \end{cases}$$

8.4.2 Authentication between elements from different armies in the SE military system

- Authentication (*X1* B, *X1* F). If a soldier from the B army wants to authenticate a F soldier, this will be done using the operation certificate, which will be verified using the F public key and the MAC address of *X*.

$$DOCxij =< j,i,sdxij,edxij,OSPi,Pkij,MACij,CALij...,Sgnxij >$$

$$XF \Rightarrow \begin{cases} drop(req) & if \quad DOC(XB) \neq valid \\ Accept(req\ ) & if \quad DOC(XB) = valid \end{cases}$$

- Authorisation (*X1* B, *X1* F). If a B soldier tries to communicate with a F soldier, then the latter will need to check the history which he receives from the OSP or a F NBBN. If the B *X* is a positive node it will be allowed to communicate directly with the F soldier, while if it is a natural node it will be allowed to do so through a F NBBN.

$$\mathrm{H}xij =< j,i,\mathrm{sh}xij,\mathrm{uh}xij,OSPi,Pkij,HPOSNij,HNATNij,HNEGNij...CLLAij,Signxij >$$

$$XF \Rightarrow \begin{cases} drop(req) & if \quad H(XB) = negative \\ Accept(req) \wedge access \rightarrow NBBN & if \quad H(XB) = natural \\ Accept(req) \wedge access \rightarrow XF & if\ H(XB) = positive \end{cases}$$

- Authentication (*Y1* B, *Y1* F). If tanks or trucks from the B army want to authenticate a F tank, this will be done using the operation certificate, which will be verified using the F public key and the MAC address of *Y*.

$$DOCxij =< j,i,sdxij,edxij,OSPi,Pkij,MACij,CALij...,Signxij >$$

$$Y(F) \Rightarrow \begin{cases} drop(req) & if \quad DOC(YB) \neq valid \\ Accept(req) & if \quad DOC(YB) = valid \end{cases}$$

- Authorisation (*Y1* B, *Y1* F). If a B tank tries to communicate with a F one, the history of the B *Y* is required and can be received from the OSP. If the B *Y* is a positive or natural node it is allowed to communicate with F tanks, whereas if it is a negative node it can do so only through the OSP of the SE.

$$\mathrm{H}xij =< j,i,\mathrm{sh}xij,\mathrm{uh}xij,OSPi,Pkij,HPOSNij,HNATNij,HNEGNij...CLLAij,Signxij$$

$$Y(F) \Rightarrow \begin{cases} Accept(req) \wedge access \rightarrow OSP & if\ H(YF) = negative \\ Accept(req) \wedge access \rightarrow NBBN & if\ H(YB) = postive \vee natural \end{cases}$$

- Authentication (*Y1* B, *X1* F). If a B tank wants to authenticate a F soldier, this will be done using the operation certificate, which will be verified using the F public key and the MAC address of *Y*.

$$DOCxij =< j,i,sdxij,edxij,OSPi,Pkij,MACij,CALij...,Signxij >$$

$$X(F) \Rightarrow \begin{cases} drop(req) & if \quad DOC(YB) \neq valid \\ Accept(req\ ) & if \quad DOC(YB) = valid \end{cases}$$

- Authorisation (*Y1* B, *X1* F). If a British tank tries to communicate with a F soldier, a history of the B *Y* is required and can be received from the OSP. If the B *Y* is a positive or natural node it is allowed to communicate with F tanks, whereas if it is a negative node it can do so only through the OSP of the SE.

$$\mathrm{H}xij =< j,i,\mathrm{sh}xij,\mathrm{uh}xij,OSPi,Pkij,HPOSNij,HNATNij,HNEGNij,...CLLAij,Signxij >$$

$$X(F) \Rightarrow \begin{cases} Accept(req) \wedge access \rightarrow OSP \ if \ H(YB) = negative \\ \\ Accept(req) \wedge access \rightarrow NBBN \ if \ H(YB) = postive \vee natural \end{cases}$$

8.5 Scenario two

As with the first scenario, scenario two assumes a military alliance consisting of two armies (B and F). In addition, new elements will be defined in this scenario (J army). Before stating how the SE provides authorisation and authentication to other nodes, some points must be clarified:

- Armies can join and disconnect without affecting the SE system.
- The public keys of the digital certificates are known by B and F elements in the whole SE system and unknown to the Japanese army.
- All nodes (soldiers and tanks) have received their operation certificates from their own OSPs (each army has its own certificate).
- Any node that is undefined and trying to operate in a different network will receive an operation certificate from its OSP and its history file will be new.
- The OSP sends node histories NBBNs.
- Each WANET has a set of policies.

To illustrate the working of the SE system and to show how the authentication and authorisation components operate between the military elements, the following example is introduced. If during a war the B army needs reinforcements from a non-NATO country such as J, in order for the J army to communicate with B forces and to engage into the battlefield, J soldiers and tanks will need to obtain an operation certificate from the OSP to perform in such situations. As J forces are non-trusted, our OSP will monitor and observe their actions based on their history in order to check whether or not J elements are acting in a normal or malicious manner. This checking is accomplished by tracing their behaviour. Usually, showing all aspects of the tracing of behaviour under the set of policies in our scenario is impossible; therefore, we provide examples showing normal, malicious and positive actions.

The following specific formalism is introduced:

Xij:	soldiers *i* from army *j*; *i* ≥1; *j* = NATO countries;
Yij:	tanks, trucks and military aircraft *i* from army *j*; *i* ≥1; *j* = NATO countries;
Z:	base station and cellular (OSP) i from SE *i* ≥1;
Wik:	soldiers *i* from army *k*; *i* ≥1; *k* = non-NATO country;
Mik:	tanks, trucks and military aircraft *i* from army *k*; *i* ≥1; *k* = non-NATO country.

In the first instance, the J will deal with the OSP. Four examples, all set in wartime, are given below to show how the OSP observes the behaviour of new nodes and the new army to build a history for every node as a basis for granting authorisation.
In the first example, if an order from an OSP has been given to Japanese troops and the soldiers obey this order, the OSP will observe these acts and decide whether or not they are normal; it will still classify the nodes as new and follow these rules:

- Authentication (*W1* J, *X1* F). If a soldier from the J army wants to authenticate a F soldier in the SE, this will be done using the operation certificate, which will be verified using the OSP's public key and the MAC address of *W*.

$$DOCxij =< j,i,sdxij,edxij,OSPi,Pkij,MACij,CALij...,Signxij >$$

$$X(F) \Rightarrow \begin{cases} drop(req) & if \quad DOC(WJ) \neq valid \\ Accept(req) & if \quad DOC(WJ) = valid \end{cases}$$

- Authorisation (*W1* J, *X1* F). If a Japanese soldier tries to communicate with a F one, the latter will need to check his history, which he obtains from the OSP or a F NBBN; if the J *W* is a new node from a new army it will be allowed to communicate with the F soldier through the OSP.

$$\mathrm{H}xij =< j,i,\mathrm{sh}xij,\mathrm{uh}xij,OSPi,Pkij,HPOSNij,HNATNij,HNEGNij...CLLAij,Signxij >$$

$$XF \Rightarrow \begin{cases} drop(req) & if \quad H(WJ) \neq DOCM \\ Accept(req) \wedge access \rightarrow OSP \, if \, H(WJ) = DOCM \end{cases}$$

In the second example, if an order from an OSP has been given to J troops and the soldiers obey it, the OSP will observe these acts and decide whether or not they are normal. If the node continues to obey every order the OSP will classify is as neutral and follows these rules:

- Authentication (*W1* J, *X1* F). If a J soldier wants to authenticate a F one in the SE, this will be done using the operation certificate, which will be verified using the OSP's public key and the MAC address of *W1*.

$$DOCxij =< j,i,sdxij,edxij,OSPi,Pkij,MACij,CALij...,Signxij >$$

$$X(F) \Rightarrow \begin{cases} drop(req) & if \quad DOC(WJ) \neq valid \\ Accept(req) & if \quad DOC(WJ) = valid \end{cases}$$

- Authorisation (*W1* J, *X1* F). If a Japanese soldier tries to communicate with a F one, the latter will need to check his history, which he obtains from the OSP or a F NBBN; if the J *W* is a natural node it is allowed to communicate with the F soldier through a F NBBN.

$$Hxij =< j,i,shxij,uhxij,OSPi,Pkij,HPOSNij,HNATNij,HNEGNij...CLLAij,Signxij >$$

$$XF \Rightarrow \begin{cases} drop(req) & if \quad H(WJ) \neq DOCM \\ Accept(req) \wedge access \rightarrow OSP & if \; H(WJ) = DOCM \\ Accept(req) \wedge access \rightarrow NBBN & if \; H(WJ) = natural \end{cases}$$

In the third example, if an order and notification from an OSP has been given to J troops and the soldiers obey this order and forward the notification to their neighbours, then the OSP will observe these acts and decide that they are positive. If the node continues to obey all orders and forward all notifications, the OSP will classify it as a positive node and follow these rules:

- Authentication (*W1* J, *X1* F). If a Japanese soldier wants to authenticate a F soldier in the SE, this will be done using the operation certificate, which will be verified using the OSP's public key and the MAC address of *W1*.

$$DOCxij =< j,i,sdxij,edxij,OSPi,Pkij,MACij,CALij...,Signxij >$$

$$X(F) \Rightarrow \begin{cases} drop(req) & if \quad DOC(WJ) \neq valid \\ Accept(req) & if \quad DOC(WJ) = valid \end{cases}$$

- Authorisation (*W1*, *X1* F). If a Japanese soldier tries to communicate with a F one, the latter will need to check his history, which he obtains from the OSP or a F NBBN. If the J *W* is a positive node it is allowed to communicate directly with the F soldier.

$$Hxij =< j,i,shxij,uhxij,OSPi,Pkij,HPOSNij,HNATNij,HNEGNij...CLLAij,Signxij >$$

$$XF \Rightarrow \begin{cases} drop(req) & if \quad H(WJ) \neq DOCM \\ Accept(req) \wedge access \rightarrow NBBN & if \; H(WJ) = natural \\ Accept(req) \wedge access \rightarrow XF & if \; H(WJ) = positive \end{cases}$$

In the fourth example, a J soldier tries to request a specific tactic from the F army in the SE using an invalid or fake operation certificate. The OSP will observe this act, decide that it is

negative and send an update for the history file to all nodes in the SE. If the node continues to behave in this way, the OSP will classify it as a negative node and adopt the following rules:

- Authentication (*W1* J, *X1* F). If a Japanese soldier wants to authenticate a F one in the SE, this will be done using the operation certificate, which will be verified using the OSP's public key and the MAC address of *W1*.

$$DOCxij =< j,i,sdxij,edxij,OSPi,Pkij,MACij,CAL...,Signxij >$$

$$X(F) \Rightarrow \begin{cases} drop(req) \quad if \quad DOC(WJ) \neq valid \\ Accept(req) \quad if \quad DOC(WJ) = valid \end{cases}$$

- Authorisation (*W1* J, *X1* F). If a Japanese soldier tries to communicate with a F one, the latter will need to check his history, which he obtains from the OSP or a F NBBN. If the J *W* is a negative node it will not be allowed to communicate directly with the F soldier.

$$\mathrm{H}xij =< j,i,\mathrm{sh}xij,\mathrm{uh}xij,OSPi,Pkij,HPOSNij,HNATNij,HNEGNij...CLLAij,Signxij >$$

$$XF \Rightarrow \begin{cases} drop(req) \quad if \quad H(WJ) = negative \\ \\ Accept(req\ ) \wedge access \rightarrow NBBN \, if \, H(WJ) \neq negative \end{cases}$$

9. Conclusion

This chapter has proposed ways to control access to a secure *ad hoc* database environment based on the history of its nodes. It also proposes an access algorithm which explains the steps taken by a node while handling requests to access a secure environment.

We have provided a case study, with specific concentration on two military scenarios in unknown and insecure territory. Scenario one assumed two NATO countries (pre-connected) in a battlefield and showed the implementation and evaluation of access to a secure environment providing authentication and authorisation between members of the same network and between other members. Scenario two considered two NATO countries with new elements (non-defined), showing the implementation and evaluation of our mechanism for allowing and preventing access to the secure environment. It detailed the access technique between NATO countries and the undefined elements, presenting a number of different situations that any military system might experience. In each situation our technique was examined to establish whether or not the situation was adequately addressed by our set of policies in order to prevent malicious acts by undefined elements in a secure military environment.

The solution is a combination of the history of the nodes and operation certificates. Each node in a secure environment is uniquely identified by its public key and MAC address. The solution addresses various vulnerability issues affecting wireless links such as active and passive attacks. The dynamic nature of networks and their membership does not affect the solution, since each node makes access decisions on its own and the use of cooperative algorithms is avoided.

10. References

Toh, C.-K. (2002). "Ad Hoc Mobile Wireless Networks: Protocols and Systems", pp: 34-37, Prentice- Hall, New Jersey,

Siva Ram Murthy, C.; and Manjo, B.S. (2004). "Ad Hoc Wireless Networks: Architectures and Protocols", Prentice Hall communications engineering and emerging technologies series Upper Saddle River,

Singh, S.; Raghavendra, C.S. (1998)."Power efficient MAC protocol for multihop radio networks", pp:153 – 157, Personal, Indoor and Mobile Radio Communications, The Ninth IEEE International Symposium .

Perkins, C.E.; Royer, E.M. (1999) "Ad-hoc on-demand distance vector routing Mobile Computing Systems and Applications", pp: 90 – 100, Proceedings. WMCSA'99. Second IEEE Workshop .

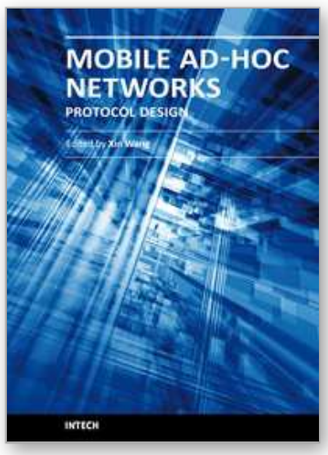
Chiang, C.; Gerla, M., Zhang, L. (1998)."Adaptive shared tree multicast in mobile wireless networks", pp:1817 – 1822, Global Telecommunications Conference, GLOBECOM 98. The Bridge to Global Integration. IEEE.

Toh, C.-K. (2001). "Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks", Volume: 39, Issue: 6, pp:138 – 147, Communications Magazine, IEEE.

Holland, G.; Vaidya, N. (1999) "Impact of routing and link layers on TCP performance in mobile ad hoc networks", pp:1323 – 1327, Wireless Communications and Networking Conference, WCNC. 1999 IEEE.

Dahill, B. ; Neil Levine, ;B. Royer E.; Shields, C. (2001). "A Secure Routing Protocol for Ad Hoc Networks", Technical report UM-CS-2001-037, University of Massachusetts, Amherst.

Hu, Y.; Perrig A. .; Jonson, D.B. (2002)."Ariadne: A Secure On-Demand Routing for Ad hoc Networks", pp:12-23, Proceedings of ACM MOBICOM 2002.



Mobile Ad-Hoc Networks: Protocol Design

Edited by Prof. Xin Wang

ISBN 978-953-307-402-3
Hard cover, 656 pages
Publisher InTech
Published online 30, January, 2011
Published in print edition January, 2011

Being infrastructure-less and without central administration control, wireless ad-hoc networking is playing a more and more important role in extending the coverage of traditional wireless infrastructure (cellular networks, wireless LAN, etc). This book includes state-of-the-art techniques and solutions for wireless ad-hoc networks. It focuses on the following topics in ad-hoc networks: quality-of-service and video communication, routing protocol and cross-layer design. A few interesting problems about security and delay-tolerant networks are also discussed. This book is targeted to provide network engineers and researchers with design guidelines for large scale wireless ad hoc networks.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Saud Rugeish Alotaibi (2011). Security of Access in Hostile Environments Based on the History of Nodes in Ad Hoc Networks, Mobile Ad-Hoc Networks: Protocol Design, Prof. Xin Wang (Ed.), ISBN: 978-953-307-402-3, InTech, Available from: http://www.intechopen.com/books/mobile-ad-hoc-networks-protocol-design/security-of-access-in-hostile-environments-based-on-the-history-of-nodes-in-ad-hoc-networks

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen