Computing and Informatics, Vol. 22, 2003, 1001–1013, V 2007-Oct-22

MANETS: AN EXCLUSIVE CHOICE BETWEEN USE AND SECURITY?

Pierre-François Bonnefoi, Damien Sauveron

XLIM, UMR Université de Limoges, CNRS 6172
123, avenue Albert Thomas
87060 Limoges CEDEX, FRANCE
e-mail: bonnefoi@unilim.fr, damien.sauveron@unilim.fr

Jong Hyuk Park

Department of Computer Science and Engineering
Kyungnam University, Masan, Kyungnam, KOREA
e-mail: parkjonghyuk@gmail.com

DRAFT VERSION

Abstract. [1] Though the MANET concept exists for decades and that many researches were carried out, such networks suffer from extremely low adoption. The main reason is the security or more precisely, the lack of. This paper defines what a MANET should be for a real use, it explains what are the security challenges and analyzes the problems of the existing proposals to secure such network. Our main assumption is that security problems as we expose them should be addressed globally and not in a fragmented manner as currently. This paper aims to define a state of the art that will be useful to propose a practical and global solution.

Keywords: MANET, Security Issues, Real Use, Comparative Analysis of Existing Solutions

1 INTRODUCTION

One of the most active research topics in the network world during this last ten years is the MANET (Mobile Ad hoc NETwork). To define briefly this appealing concept, these networks are truly peer-to-peer networks where each node uses wireless communication means. Unfortunately, today, they are not used in real life or only in very few dedicated contexts as we will illustrate quickly below. Why such a nice concept is still not commonly adopted? This question is the discussion thread of this paper. The main reason is the lack of security to achieve the same level than that provided by common network (even that based on wireless network – WLAN – with the use of cryptographic tools like WEP, WPA and so on). The aforementioned MANET already deployed are still used in very restricted contexts. For example, only ad hoc network between two or three computers in a room or a building could be easily deployed by cooperating users with some sufficient security. But this model could not easily scale into a MANET, where mobility and appearance/disappearance of nodes occur very frequently and where users cooperation could not be enforced. Sometime, cooperation could be achieved (for example in a conference theater) and could spontaneously lead to a large wireless network but often in this case, security is not a concern. Once again, it is not a really mobile network but rather a "fixed" network. These two small examples do not want to be exhaustive but they illustrate with real life scenarii a summary of the contexts of use and of their specificities (e.g., not mobile for both examples; secure and small network for the first example; not secure and larger network for the second example).

The aim of this paper is to define clearly what a MANET should be for a real use and what are the security challenges to solve regarding the problems of the current existing solutions. To achieve this goal, section 2 will expose the underlying concepts that characterize a MANET. Section 3 will analyze the existing solutions attempting to secure the MANET and will exhibit their security weaknesses. Then we will conclude our comparative analysis and the perspectives to secure the MANET will be drawn in section 4.

[1] This research was supported by Kyungnam University, Korea.

2 DEFINITION OF MANET AND REQUIREMENTS FOR REAL USE

By definition, a Mobile Ad hoc Network (MANet) is a network created in a spontaneous manner and composed of autonomous and mobile elements (laptop, PDA, smartphone, UMPC, tablet PC, etc.). It is not supported by a *preset infrastructure* and thus, it does not have a clear boundary, so, the network could only be defined by a set of elements sharing the *same goal*. To enable this spontaneousness and this mobility, these elements generally use wireless communications (Bluetooth, WiFi, etc.) and operate on battery. Mobility and wireless communication are not sufficient features for characterizing an ad hoc network. Sometime, mobile workers get access to their company network though wireless communication like WiFi or cellular phone network. To ensure that this access does not harm the company network a solution requires secure access to a quarantine network zone. Generally, this secure access relies on ciphered communication and strong authentication procedure like some based on the use of certificate and PKI (Public Key Infrastructure). In this case, the wireless and mobile implemented network is not ad hoc and represents only a continuation of a regular network (the only gain is a wireless link that allows mobility). An implementation of such a *continuation of a regular network* is MobileIP [1] which provides solution to mobility with a model based on the use of a "Home agent" element to relay communication between a peer and the current mobile element (the node appears as belonging to its original location in order to establish new communication). Some security is provided by the use of IPSec (relying on PKI to authenticate and set up secure channels with IKE). MobileIP gives an implemented solution to mobility of nodes but it does not give any mechanism to organize spontaneous and large MANET (that requires multi-hop communication).

From this assertion, we have to consider that infrastructure is not only hardware based but also software based and that mobility and wireless communication are not the only features to define a MANET.

2.1 No Preset Infrastructure

An important characteristic of the mobile ad hoc networks is the total absence of preset infrastructure and all communication between nodes are provided only by their wireless connectivities.

By definition, the infrastructure of a network is used as support for the activity in this network: it makes possible the exchanges (definition of interconnection paths) and set up mechanisms ensuring the security. In the traditional "wired" networks, the infrastructure is made up by a physical part (hardware – links and interconnection boxes) and it can be supplemented by a logical part (software – like VLAN, VPN, PKI, DHCP server, etc.). Some of these logical means represent a centralization compared to the network: all the elements of the network must be able to join frequently dedicated servers (for example, to the Certification Authority in the use of PKI). However this approach is essentially contradictory with the volatile nature of the MANET and so, it could not be sufficient to provide the expected security requirements.

In MANETs, the infrastructure must enable the communication between all the elements belonging to the network, i.e. to enable the establishment of paths for the transfer of the messages between the elements. These paths cross the elements because they are the only ones being able to forward a message between two elements when they cannot communicate directly since they are outside of the radio coverage (requiring routing algorithm). Thus, we consider that routing algorithms are part of the infrastructure of an ad hoc network.

2.2 A Common Goal

The most commonly accepted view of ad hoc network is to consider them like open system with people freely enter or leave the network according to the range limitation of their radio. This simplistic view could only match the model of single hop network where all elements access the same communication channel (communication occur only between nodes within radio range from each other). When a communication requires transfer through a third party node, some cooperation must be achieved. This cooperation relies on a minimal condition: sharing a common goal. This goal must be shared by users themselves and must be translated through the user level to the hardware level.

In general, the ad hoc networks have a goal shared by the elements which compose it: at a low level, this common goal consists in enabling the data exchanges and the resources sharing between these elements of different nature and capacity. This sharing is carried out according to roles given to each element which make it possible to organize the access and the use of a resource (for example it is possible to identify which node acts as a server and as a client as well as which node is granted to use it). At a greater extend, this goal is organized by an administration which makes it possible

DRAFT VERSION

to translate the human intention of the cooperating users (i.e. the security policy like the definition of the border of the network and the access rules to the resources).

2.3 Lifecycle of Mobile Ad Hoc Network

In a general manner, a regular network has a lifecycle. Before its existence, it is planned, i.e. administration and infrastructure are defined by taking into account the goal of the network and the functional needs. This planning can be the result of a negotiation between all the users or entrusted to a restricted number of privileged users (in this latter case, a centralization is implicitly needed). Then, during the lifespan of the network, the administration can be dynamic or not (evolution of the security policy, by addition or withdrawal of elements, or by the reconfiguration of the resources sharing). Note that it is also possible to start again a planning phase to create a new instance of the network provided with a newly defined administration while integrating the chosen elements of the previous network. Nevertheless, this approach requires a new centralized process without the participation of expelled nodes.

In the case of an ad hoc network, the infrastructure (as shown in section 2.1) and the administration must be supported by the elements themselves. Consequently, the definition and the application of the security policy depend on each element and, the administration is distributed by nature. In the same way, the mobility of the elements makes extremely dynamic the infrastructure: the topology of the network changes quickly and in a random way (appearance/disappearance of nodes present or not at the starting of the network, modification of the communication links). Under these conditions, any approaches of centralization must be prohibited since the access to a group of selected elements may not be guaranteed during the lifespan of the network (for example the group hosting an authentication server).

Moreover, the administration uses the management of the identities in order to define the border of the network and to regulate the resources sharing. These operations must be in conformity with the security policy to which the users belonging to the network must adhere and conform. That also imposes that each element of the network is equipped with its own or a shared identity which leads to several security problems that will be discussed later in section 3.1.

2.4 Peer-to-Peer Network vs MANET

Peer-to-peer network is very similar to ad hoc network. They share a lot of essentials characteristics and seem to take over their counterpart. They took the mainstream and a lot of companies struggle to turn them into successful business model as Skype for VoIP or Joost for TV broadcast. The success of p2p networks put the shame on the minimal adoption of ad hoc networks and worst on MANETs. They seem to engulf all desired promises of ad hoc network: benevolent people accepting to support network by supplying resource sharing, commitment for being online as long as possible, etc. Nevertheless they diverge strongly from their very own purpose: in existing p2p network (e.g., Kazaa) the most successful and appealing feature is to give users access to assets that users do not possess (like not legally authorized contains exchange: music, video, commercial programs, etc.) or that one user wants to share with the highest number of people (like an artist with his work, or TV shows embedding advertisement, etc.) in order to gain the biggest possible audience. As aforementioned in section 2.2, we believe that the only one context that could lead to strong adoption of the MANET is that of collaborative work where assets are possessed by users and should be only shared by people taking part in this work. This discrepancy about purposes explains why avoiding selfish behavior, security of exchanges and identities must be enforced in ad hoc networks (in p2p, anonymity is a strong requirement at the contrary of ad hoc network where privacy prevails) as we will present this below.

2.5 Security Policy

The security policy must guarantee security fundamentals: authentication, integrity, confidentiality, non-repudiation and availability. The nature of the mobile ad hoc network implies new risks in particular related to elements of the network themselves since they provide the infrastructure, and new undesirable behaviors are highlighted: selfish behavior in addition to the malevolent behavior. It should be noted that these undesirable behaviors may be out of the responsibility and will of the users and may be caused by virus, malware or even faulty operations at the level of the operating systems or applications of the mobile node. Thus, these nodes must not be trusted and some facts must be taken into account for the mobile ad hoc networks:

DRAFT VERSION

- the element itself provides its identity(ies). Consequently it is difficult to guarantee uniqueness and to prevent the impersonation of an element by another one;
- each element provides the support of the network, in particular it runs itself the needed algorithms. Thus the element is able to modify these algorithms;
- the element, mobile by nature, operates on battery what limits its autonomy and makes it less voluntary to ensure the support of the network: power consumption to the profit of the others and not for itself. This exposes a new improper behavior: selfishness;
- the power saving functions as well as the mobility of the elements induce the appearance and the disappearance of the elements. Thus it is necessary to be able to distinguish its normal behavior from a selfish one.

To overcome the problem of a node that refuses to route the messages in order to save its battery or because it is malicious, some kind of infrastructure must be introduced into MANET. This infrastructure should contractualize that all nodes perform their best in order to support the network requirements, like routing, and ensure some other fundamental properties to guarantee the security of mobile ad hoc network, i.e. the security of the identities and that of the routing algorithm. In our opinion, such an infrastructure should rely on a secure system installed on each node. To convince the reader of this fact the next section analyzes the existing solutions for securing the MANETs without relying on a secure system and we will exhibit their weaknesses.

3 SURVEY OF THE EXISTING SOLUTIONS FOR THE MANET SECURITY

In this section we present the main existing solutions aiming at ensuring the security of the identities and at enforcing the support of the network (e.g., routing algorithms in multi-hops network).

3.1 Security of the identities

In the case of an open network and where communications are done between elements that connect to others randomly, the identity cannot be necessary; on the other hand the identity is necessary for example when one wants to be able to point an element to communicate with it, or to select the elements being able to take part in the network. This identity is difficult to apprehend because it can be considered according to very different points of view like that from the user compared to that of the hardware. By definition, an identity must present a certain number of properties: it must be single, non-repudiable, non-transferable and invariant [2]. According to the applications and the expected level of security, some of these properties are necessary and some others could be ignored. There exist many proposals to ensure these properties. It is possible to evaluate them from the point of view of security offered, but also according to the type of ad hoc network that these proposals allow (planned or not, centralized or not, managed dynamically or not).

The identity makes it possible to manage the elements in a set composed of different and independent entities (human group, data-processing network, etc.) while allowing to individualize them or at the contrary to gather them. To have an identity is mandatory to apply a security policy, in particular to observe the evolution of the behaviors of the elements in the time (evaluation in agreement with the security policy). To be able to be used within the network, an identity must either exist a priori, or be created in accordance with the properties which it must exhibit. Lastly, it is possible to bind identities between them according to the needs, for example to express the membership of an element to a group or to a network. It is desirable that this is done so that all or certain properties of an identity can be found in the related identity. Then three fundamental operations on the identities can be distinguished: *creation, diffusion and association.* It could be necessary to examine if a property is kept or lost through the application of one these three operations. For example, if a user has been previously associated to a network identity (through the creation operation) and joins again the same network after leaving, it could be necessary to prevent the association of this user to a different network identity in order to guarantee the properties of non-repudiation and non-transferability (i.e., spoofing). In the case of defining security policy, one security requirement could be uniqueness of the creation of a network identity based on a intrinsic identity of the user of the node (hardware identity related to legal identity); another requirement could be that network identity must be non-transferable and non-repudiable (one node has a single immutable identity during the lifespan of the network). These operations can be used at various stages of the lifecycle of the network in a distributed or centralized way.

The objectives of security are double: to make sure that an identity has the required properties and that all handling operations of an identity are in conformance with the selected security policy. If

LAB VERSION

one wants to be able to make evolve the security policy and in particular the border of the network, it is necessary that these operations can take place throughout the life of the network (identity management).

The ad hoc characteristic of the network increases the difficulty in making secure the identity management. A solution to reduce this difficulty can be to limit the use of some of these operations to certain phases of the lifecycle of the network and/or to introduce centralization (one or more elements of the network must be assigned to specific tasks – even if it is contrary to the concept of ad hoc network).

In a wired network, the problem of the diffusion of the identities is partially solved by the use of directory like a LDAP server based on X.500. By combining this server with the model of security based on asymmetrical cryptography, certificates and certification authority, one makes secure the operations of creation and association of an identity to an element, but one also guarantees the properties of each created identity namely uniqueness (use of cryptographic asymmetrical keys that are truly randomly generated), non-repudiation and non-transferability (each identity are associated to a unique public key in a document in a standardized and interoperable format that is signed by a trusted third party (TTP), avoiding any modification without agreement of the TTP. Impersonation is avoided by authentication: the use of a challenge to give proof of the possession of the associated private key). This is a well-known model of PKI, that relies on an enrollment authority and a certification authority to manage identity. Lastly, the possibility of revoking a certificate makes it possible to remove an association to prohibit the network access to an element, or to put an end to the existence of the whole network.

Into an ad hoc network, the need for a server representing the TTP, introduces several problems: the first is when network identities are created; the second is when the trust must be ended.

The first problem is how to trust a TTP. This trust must be ensured at all levels, from the way to contact it (identity, location and data exchange) to the soundness of its treatment. A common problem with the use of a TTP is the impossibility to detect a malevolent behavior of the TTP. This problem is a order of magnitude more intricate to solve when the TTP has to be located within a MANET. In the case of a PKI, the certification authority could issue two certificates for the same identity due to a malevolent behavior or a lack of security process during the enrollment process. Worst, the TTP and the enrollment process could be distributed onto a set of nodes, leading to a globally non-secure setup due to a partition of the network (one node could enroll itself under a certain identity into a subpart of the network, when the same identity is used by another one into another subpart of the network) or also a malevolent behavior. If one can find two valid certificates issued by the same CA as TTP, that could be difficult to conclude.

The second problem is translated in the centralization and availability problems: in the case of PKI, the revocation list must be constantly available for checking, like precondition to any communication between elements.

There are various proposals to try to solve these problems as we will present them below.

3.1.1 Proposal 1: Low centralization with some kind of TTP

The objective is to diminish the need of centralization keeping some kind of TTP.

A solution is to multiply the CA servers.

Distributed Certification Authority, Threshold Secret Sharing Several methods of distribution of the certification authority were proposed, based on scheme of threshold cryptography (polynomial, additive or combinational): the private key of CA is divided on a set of N nodes and to rebuild a certificate signed by CA, it is necessary to get K, with $K < N$, partial signatures. There are several protocols of partial signatures with RSA keys [3, 4, 5, 6]. These methods make it possible to let an element joining a group according to the decision of a group at least K nodes. On the other hand, they require the availability of at least K nodes and are generally applicable only to small size networks. In the solution [7, 8], DSA is used instead of RSA. The distribution can be partial [9, 10] or total [11, 12]. These solutions are interesting from a cryptographic point of view but do not provide much of help to diffuse secured information for identifying and contacting one of the N servers, and could only provide better flexibility.

A solution is to limit centralization to occur only during the phase of planification.

Shared Secret This proposal aims at defining a border for a network without distinguishing the elements from the network from/to each other. The solution consists in having a shared secret between all the members of the network. Thus, this secret makes it possible to exclude the elements which do not know it. If one would like to define subsets of elements, the method is similar, i.e. that

DRAFT VERSION

it is necessary to share a new secret between the only members of this subset with the exclusion of the other members of the current set which one belongs. That can correspond to a new phase of planification if one wants to make evolve the border of our network. Moreover this shared secret must be exchanged between the elements in a protected way, what throws a problem since there is not already secure network to do it (thus, it will be necessary to use mechanisms similar to pairing). Lastly, it will be noticed that a node cannot communicate with a subset without belonging to this subset. Thus, this shared secret holds the role of an implicit and mutual identity for all the members of the network and can be compared to an identity for the network. The phase of sharing of this secret occurs before the existence of the network, i.e. in the phase of planification, which is against the spontaneous nature of an ad hoc network. This shared secret is tightly bound to the life of the network: if it happens that it is revealed in an accidental or malevolent way then the network does not exist any more, its border disappearing (this is just a matter of theory because elements cannot all be warned to stop using this secret). In the same way, if it is possible to integrate a new element by revealing the secret to it, it is impossible to reject an element without having to create a new network based on a new shared secret by finding the means of excluding this element. This could be a frightening problem if all nodes could not be contacted in the case of partitioned network.

If an identity should be provided to each node, the security of the association of an identity to an element goes by the verification that the element is entitled to provide it as being its own. This verification can be done by the detention of a secret which will prevent whoever who does not have it to adopt this identity, but there is no way to associate this secret to the network secret.

A solution is to use a PKI but with a limited need of connectivity.

MANET-ID To solve the problem of the access to the list of revocation and to avoid its often distribution between the elements (what throws important problems in a network where topology frequently changes and could create many partitions), it is proposed in [2, 13] to use certificates with a very limited lifetime in order to constraint the elements to periodically obtain a new certificate from CA. The solution that they recommend is to use an access to the server hosting the CA by a direct communication link like a connection using cellular phone network (GSM/GPRS connection), which is not easily acceptable in the case of a pure ad hoc network.

A solution is to use a PKG (Private Key Generator) that could be duplicated.

IBE This problem of ensuring flawless work of the TTP in a MANET arises also with IBE [14] where network identity is defined by a PKG server (Private Key Generator) using a secret and some public information provided by the user of the node. If the PKG is distributed on different nodes, the duplicate network identities problem could occur. A solution has been given by the Certificateless Public Key Cryptography where Elliptic Curve Cryptography has been used to allow the user to add his own secret to the process of obtaining its public key and private key. So, the process used two secrets, one for the PKG and the other for the user. Duplicates identities are thus no more possible, nor direct malevolent behavior of the PKG. Besides this, the possibility to independently infer the public key of a node knowing its public identity could not be achieved anymore. Thus, the public key of a node must be diffused prior sending any ciphered message.

3.1.2 Proposal 2: Strongly distributed without any TTP

There are other proposals aiming at avoiding the PKI model. Often, they offer degraded or even non-existent versions of identity management and consequently limit the administration possibility of the setup network.

It is possible to consider the chain of the identities for an element of the network according to the levels: hardware, then software and then user. It seems natural to wonder about the possibility of defining the security according to this chain, on the basis of the simple idea that a given hardware belongs to a given user and that the application is under the control of the user. It can then be possible to have a single identity for all the levels by using that available a priori. Often, the elements used in an ad hoc network are equipped with a network card and a communication stack enabling them to integrate a traditional wired network; they can have a certain number of hardware or software addresses. Indeed, to be able to communicate in a network, an entity must be identified by a single address in the considered network: the goal is to be able to identify the partners involved in a communication. Some of these addresses are given a priori, for example during the construction of the hardware or configured directly by the user or indirectly by another element (server of configuration).

A first proposal is to use the layer 2 and 3 addresses of an element according to the OSI model as an identity.

DRAFT VERSION

OSI layer 2 address The first approach is to give this address to the element at the construction time. The physical address or MAC, "Medium Access Control", composed of the identifier of the manufacturer, OUI, "Organization Unique Identifier" and of a unique identification number for the interface chosen by the manufacturer. This association is supposed to identify in a unique way the communication hardware. Moreover in Bluethooth, MAC device address takes part into the pairing process and the construction of link key. However, this address can be easily duplicated or modified. This situation can result from an error on behalf of the manufacturer, but also of the use of software tools with malevolent intention. It thus does not guarantee any of the properties expected for an identity. It is also not possible to get access to the outside of the network (single hop address).

OSI layer 3 address One can notice that in the case of a wired network, the elements need at the same time a physical address and an IP address. This IP address can be selected in a range of private addresses (in this case there will be no communication outside the built network) or chosen in a different way if one wants to belong to Internet (attribution of the address by a NIC, "Network Information Center"). The diffusion to the elements can be manual or automatic (DHCP server, "Dynamic Host Configuration Protocol" or a combination of MAC address and network prefix sent by a router in the case of IPv6 [15]).

In general, an element needs several addresses according to the context of the communication: if it takes place within the same link of communication a single and unique address on this link is sufficient; if it takes place between two different links of communication, it is necessary to have an address combining the identity of the link of origin (or destination) at a single address on this link (interconnection of at least two local area networks).

In the case of an ad hoc network, an address of interconnection is not mandatory and can be difficult to define without requiring cooperation from all the nodes of the network. The element could only obtain a single address on the link of communication which it reaches at the time of its initialization (like the model of access to the same communication channel with single hop exchange only).

OSI layer 3 address with IPv6 autoconfiguration This approach is to allow the element to choose its own address on the local link, by checking that it is not already chosen by another element (indeed, the consultation of the members of the network is needed to be sure that the address is not already used, this process is conducted by the "neighbor discovery protocol" of ICMPv6). It is the principle of the autoconfiguration of the identities in IPv6 (Local Link Address). Therefore, this address can be easily duplicated or modified. This situation can result from an error on behalf of the manufacturer, but also of the use of software tools with malevolent intention.

The previous solutions could only provide uniqueness but do not prevent repudiation, transferability and impersonation. Thus we have to use cryptographic tools to ensure some of these properties.

IPv6 and SUCV (Statically Unique, Cryptographically Verifiable) Another proposal is to use the capacity of the IPv6 addresses and the asymmetrical cryptography to define the address of local link of an element based on its public key. Thus, the address is guaranteed unique thank to the property of uniqueness of the public/private keypair [16] and the process used to derive a part of the address from the public key [17] in order to obtain an address length of only 64 bits. This address is not transferable or more precisely it cannot be impersonated without possession of the related private key. Nevertheless, this proposal does not prevent the element from having several addresses which it can decide to give up. Indeed the non-repudiation property is really important to trace back and punish the element exhibiting a bad behavior. This proposal has the merit to enable the distribution of the operation of creation. On the other hand it does not offer security for the operation of diffusion: these identities must be known between the elements before their use, and consequently the administration is only possible during the planification phase of the network. The possibilities are very similar to those presented in "shared secret" based model.

3.1.3 Proposal 3: Less distributed: self organizing "Web of Trust" – Social networking

Another proposal consists in establishing networks of trust, where each element could serve as TTP for other elements giving them warranties about identity of one node. This model establishes a network of confidence or a "Web of Trust" where a path of trust leads from one trusted node to another one. The idea consists in using the model suggested by PGP, where chains of certificates are established between the elements. In [18], it is noticed that a small number of certificates is sufficient

DRAFT VERSION

to be able to check the links of trust from a new element towards an element whose confidence was established beforehand.

To mitigate the problem of the availability of the nodes, solutions as in [19, 20, 21, 22, 23] propose the self-generation of a keypair and a certification by a trusted node. These methods present the advantages which the authentication relies only on local information between nodes and are completely supported by spontaneous, not-managed, not-centralized networks. On the other hand, in addition of the problem of need for a certain "density" of the network, it is the system of trust on which these methods rely that only enables it to bring a very limited security.

Unfortunately, it does not prevent the malevolence, because once a certificate have been digitally signed by one node it could be spread to the whole network as much copies of itself as needed, and needed modifications to remove the proof of trust from a certificate requires to spread again the new modified version to each node (the problem is that it is the certificate itself that embeds all trust guarantees).

For the initialization and for the first exchanges, certain solutions propose to get the key from an element in secure way by a parallel communication channel such as an infra-red link: the public key is exchanged by the network then a checking is made by the direct exchange of a hash of this key.

In the model of the sub-group of trust, all the members of a group trust each other and if two nodes want to be identified, intersections between these groups are sought to create paths of trust. The constraints are that it is initially necessary to establish trust within a group and that a lot of different established relations between nodes are needed. This solution is studied in [24].

3.1.4 Proposal 4: An hybrid solution: strongly distributed and a special kind of TTP

We have seen that a distributed or duplicated TTP could not be prevented to behave incorrectly, so, this solution proposes to use a secure process environment that could embed TTP operations and secret (e.g., master keypair in the case of a PKI).

Based on smart card This solution [25] is based on the possibility to define two strictly independent phases according to their respective destination, during the lifetime of the smart card. The first phase occurs during the mass production of the smart cards, from factory to the customer (personalization phase: installing applet on Java smart card, data, cryptographic means, etc.). After this stage, all the smart cards could be virtually the same in regard of capabilities and of embedded data according to the requirements of the customer. This customer could be a global structure like a broker with the only purpose of designing and selling these smart cards to end-users. The provided services are to allow each user to define his identity solely with his smart card. This is the second phase where identities are created using the smart card issued from the first phase according to the need of the end-user. The provided identity is non-transferable, non-repudiable and unique according to the applet used to generate it and using the smart card as secure storage (tamper resistant). The smart card provides also tools to establish secure channels with another smart card of the same kind in order to exchange identity, or to authenticate user against his already defined identity (preventing usage of stolen smart card). Thus, the TTP is distributed on each smart card that should be used on each node, and each user has warranties that himself and all others users are dealt in the same manner by all the smart cards (same executed applet). Process and security being the same for all,the trust could be established. The fact that purposes of defining the smart card and using them are strictly independent ensure the soundness of the proposal (complicity are not possible if the smart cards are mass produced and manufacturer could not target specific user during the personalization process).

DRAFT VERSION

3.2 Security of the support of the network

Once the stage of authentication succeeds, an entity has access to the network services: it gains in particular the right to legitimately take part in the essential functions such as the routing.

3.2.1 The participative or collaborative routing

In an interconnected network, the construction and the maintenance of the infrastructure supporting the multi-hops communications are ensured by the process of routing. Its role is to define optimized paths in order to maximize metric defined by the community (time, paths length, paths stability, etc.) for the routing of the data of one source towards one or more recipients. It is generally characterized by two operations which are the exchange of control message to construct route and the forwarding

of the data. The first operation aims to obtain a representation of the topology of the network then to compute and maintain paths, using information exchanged between the entities (state of links, vector of distance, paths towards the source, etc. according to the type of routing protocol). The second operation aims to ensure in a transparent way the forwarding of the packets of applicative data from end to end. Within the framework of the wired networks, the existence of an infrastructure of communication (the set of dedicated physical and software entities, independent of the users, and controlled by a legitimate authority: e.g., routers, etc.) enables to ensure the sound application of the routing process and thus the well behavior of the network. At the contrary, the ad hoc mobile networks are characterized by an absence of separation between the functionalities of management (i.e. administration) and use of the infrastructure of communication: the entities are an intrinsic part of the infrastructure. Thus, to pass beyond the limitation of their radio range, all the entities must take part themselves in the process of routing.

3.2.2 Profiles of the elements

In the majority of work on the routing protocols in field of ad hoc network, it is supposed that the entities are altruistic, i.e. they are fully co-operative and that they honestly take part in the operations of routing which fall to them. However this assumption is debatable in an environment without rule and preset referee, where the resources are limited and where the multiple entities are a priori independent/autonomous and with divergent individual motivations. We distinguish two main reasons which lead an entity to adopt a contrary behavior with the operation of the routing: selfishness, ill will and failure.

Selfish element Because of scarcity of the resources, a selfish entity is concerned with its power consumption and it does not wish to serve the network (i.e. other entities). Its main objective is to maximize its individual profits: to use the network services offered by the other entities, while contributing to it the least possible. Its behavior is characterized by a non-participation in the routing operations of the messages.

Malevolent element A malevolent entity aims at intentionally harm the sound operation of the network. To achieve this goal, it can obstruct the basic operations of the routing, and if some kind of protection mechanisms has been set up, it will seek to make them inoperative (e.g., by bypassing).

Failing element The failing entities behave in an egoistic way or sometimes malevolent for reasons of internal errors (e.g., bad configuration or hardware fault), or external (e.g., interferences, collisions). In short, they do not conform to the specifications of the protocol.

Sometimes nodes could switch from one behavior to another.

3.2.3 Few attacks against the support of the network and the existing proposals

The routing protocols in the ad hoc mobile networks are likely to have vulnerabilities in their control message exchanges phase and in their forwarding phase.

Control message exchanges phase

Vulnerabilities A malevolent entity can compromise the integrity of the representation of connectivities (states of links) of the network, due to the diffusion of fraudulent information in the control message exchanges phase (by handling incorrectly or forging of the static fields such as the identifier of the source, the identifier of the recipient, the number of sequence and the mutable fields such as the path towards the source, the number of hops, etc.). Consequently, the traffic is potentially diverted and the whole performances of the network are degraded.

This could be used to disturb the network to the extend of shutting it off. This could also be used to abuse from remuneration based system by modifying proof of support of one node involved in the chain of transfer of a message (suppress an intermediary node for example).

Security Goals The first challenge of security is to guarantee the integrity of the information collected by multiple entities in the control message exchanges phase. One needs:

- to prevent that an external intermediate entity to the network can take part to the control message exchanges phase;

DRAFT VERSION

- to prevent that each legitimate intermediate entity in the network modifies the static fields of heading control messages;
- to ensure the conformity of the modifications of the parameters according to the specifications of the implemented protocols.

All these goals lead to protect the execution of the routing algorithms.

Existing proposals

- External attacks against control message exchanges phase. Sanzgiri et al. proposed the protocol ARAN (Authenticated Routing for Ad hoc Networks) [26] which plans that only the entities in possession of the cryptographic means can authenticate information of routing coming from their neighbors, the other entities being excluded. Although the protocol protects routing information against the external attacks, the various hostile behaviors of the entities due to the nature of the environment are not taken into account in the security objectives: e.g., the case where a legitimate entity fraudulently modify this information is not examined. In addition, it assumes the existence of a TTP for the management of the keys, which lead to a non-desirable centralization.
- External and partially internal attacks. Papadimitratos and Haas proposed a protocol of secure routing for DSR [27] which guarantees the integrity of the information of connectivity exchanged from end to end between two entities (source and recipient) by means of Message Authentication Code (MAC) during the phase of path discovering. However, the protocol makes the assumption of the existence of an infrastructure of key management to establish a protected association (exchange of shared secret) between the source and the recipient. The protocol is not immunized against the attacks by blackhole and rush (all the exchanges from the source towards the recipient can be faded and new route requests could be dropped due to duplication). It can be noticed that there is again the same problem: it is not because the source and the destination share a secret to secure their exchanges that they can trust each other for their respective behaviors concerning the correct realization of the routing operations. This protocol does not protect the fields of information of a RREP packet (Route Response Packet used to reply to a demand of route discovery in an on-demand algorithm), which would make it possible to a recipient to modify it, and in particular to add to the packet the entities with which it would be in collusion. This could lead to very powerful attack.
- External and internal attacks against control message exchanges phase. Hu, Perring and Johnson proposed ARIADNE [28], a secure reactive routing protocol which uses the protocol of authentication TESLA and a chain of hashes to prevent that an intermediate entity takes the identity of another and modifies, by suppression or insertion of entities, the path towards the source (i.e. mutable fields). The protocol is based on the division of a secret between the source and recipient entities, and on a synchronization of clock (for TESLA).

All the approaches (of secure routing) presented propose mechanisms to authenticate the operations of control message exchanges phase of the existing routing protocols such as AODV and DSR, and rely on the use of a symmetrical or public key cryptographic system (cryptographic tools dedicated to the routing). They make the assumption that a pre-deployment distribution of the shared secret on the whole of the entities (for a network of size N, each entity will have to store $N * (N-1)/2$ secrets), i.e. the assumption of the existence of a centralized trusted third party dedicated to management of the keys. In addition, the objectives of security of these proposals are to fight against the attacks in the control message exchanges phase, but they remain inoperative against the attacks in the forwarding phase (the adversary belonging to a path).

DRAFT VERSION

Forwarding phase

Vulnerabilities The forwarding phase is vulnerable to the following attacks: by modification (of the contents of the data); by deletion (can be seen as a deny of service); by replaying the traffics having to be retransmitted. Some examples of attacks are the blackhole, the grayhole, the wormhole, rushing [29].

Security Goals The goals of security is to prevent user to get access to the inner part of these algorithms in order to modify them or their data. Another security goal is to ensure the continuous availability of the network, i.e. ensuring that a node could communicate with another one if a physical path exists between them. Other goals are to provide expected security as provided in

regular network. In the case of ad hoc networks, limited computation power and very fast evolving topology lead to the need of reinforced cryptographic use by frequently changing the keys used to secure all exchanged information. Thus, these issues must be carefully addressed by using dedicated cryptographic algorithms ensuring the PFS/PBS (Perfect Forward Secrecy/Perfect Backward Secrecy).

Existing proposals In order to motivate nodes to support the network and to share some of their resources to other nodes, mechanisms have to be implemented. This different mechanisms use incentive or threat of exclusion to get adherence of the nodes or, sometime game theory to stimulate a gamer winning behavior.

- Sprite. Sprite (A Simple, Cheat-proof, Credit-based System for Mobile Ad Hoc Networks) [30], Zhong et al. propose a scheme to enforce collaboration between nodes without requiring dedicated tamper-resistant hardware on each node. They use results of game theory in order to prove that cheating can be avoided, making it a non-valuable choice for a node. Their approach requires that a centralized service, the "Credit Clearance Service" (CCS) must be accessible from each node in order to reward it for its support to the network. This centralized service can be only provided by a server located outside of the ad hoc network. Sometimes when the CCS could be contacted with a sufficient bandwidth all receipts used to prove that a node has forwarded a message are sent to it. The CCS server can examine all this receipts in order to check them and to give back to nodes their rewards.
- Reputation. To protect the forwarding phase of the packets of the routing protocols, reputation systems based on the observation and the control of the traffics network were proposed. The work described in Watchdog and Pathrater [31], CORE [32] and CONFIDANT [33] uses mechanisms to assign a value of reputation to the entities of the network in order to quantify their degree of confidence in their behavior with respect to the operation of data forwarding. The entities of which the degree of confidence is weak, are completely excluded of the routing or are avoided at the time of the definition of the paths.

  In their models, each entity locally observes the exchanges of messages of its neighbors, and checks that there is no deviation between the diagram of communication observed and that expected by the system. Any deviation is regarded as an anomaly of behavior which degrades the reputation of an entity. To solve the problem of the training of the values of reputation of the entities that can not be directly contacted, CORE and CONFIDANT propose a mechanism of alarms or recommendations exchange (positive for CORE, negative for CONFIDANT).

  The behavior of the aforementioned mechanisms relies on the strong assumption of a shared communication channel, allowing the listening of the whole traffic network in the radio coverage, but this is not always possible. In CORE and CONFIDANT, the ill will attacks against the mechanisms of protection themselves are not fully taken into account. They are vulnerable to the compromising of the code and the exchanges of recommendation (i.e., discredit/slander of benevolent entities, over-estimate of malevolent entities). CONFIDANT proposes the use of bayesian statistics to restrict the harmful effects of false alarm and calumny.

  Therefore, since the problem of the uniqueness of the entities is not tackled, an entity can change its identity to get rid of bad reputation or to create multiple virtual elements to increase its own reputation. In this context, any attempt at charge of ill will acts to a particular element is made impossible!
- Remuneration. Within the framework of the Terminodes project [34], Buttyán and Hubaux proposed a distributed mechanism of remuneration based on the exchange of virtual currency (called Nuglets [35]) which aims: to stimulate the participation of the nodes in the operation of retransmission of the packet in the routing process; to discourage the nodes to overload the network.

  It is interesting to describe the exchanges, by specifying that authors assume that paths are established between the nodes: when a node sends a packet, it gives the nuglets related to the cost of retransmission induced by the intermediate nodes implied in the transaction; when a node forwards a packet, it accumulates nuglets.

  To ensure the security of the remuneration mechanism and to avoid any fraudulent handling of the meter of nuglets, each node is provided with a protected environment of execution. This environment is used as protected storage for: the cryptographic tools (pair of public/private keys of the security module, keys of session) used to authenticate the exchanges of packets; the local meter of nuglets of the node.

DRAFT VERSION

It also makes it possible to carry out in a protected way the operations of payment (credit/flow).

One can note that these algorithms treat only the operation of forwarding, and depend on the good behavior of the operations of control message exchanges phase for the establishment of the paths. To solve the problem they propose that those operations are carried out in the protected environment. This protected environment of execution being hosted by a node in charge of managing network connection, it would be necessary to ensure of the security of the communications through this node. The participation of the elements is not imposed by the system during the life of the network: the mechanism is not protected against ill will where the underlying motivations of the elements are not any more to maximize their personal profits obtained by the use of the network but to maximize the damage caused to the network. More subtly, some well-defined acts of ill will would make it possible an entity to benefit from the network while taking part only in flows for which it carries interest.

3.2.4 "Routing-free" networks: Delay Tolerant Network

There is another kind of MANETs that reduces the stress on algorithms dedicated to the support of network by removing the need to define a route to the recipient of a message. This kind of network is called DTN, Delay Tolerant Network[2]; it relies solely on spreading a message. Thus no warranties are given on the success of reaching the recipient neither on a upper limit for the delay in order to conclude to a possible failure. DTNs complexify the problem of identities management in particular for the ability to distribute them on each node. The security of message content requires also strong tools and a lot of researches are conducted to address the dual cryptographic requirements of PFS and PBS.

4 CONCLUSIONS AND PERSPECTIVES

In this paper, we have shown that even if the MANET concept exists for decades its adoption for a real use is very low due to the lack of a global security solution. We have clearly defined what should be the characteristics of a MANET in such a context. An analysis of the main existing proposals to secure the MANET has been conducted and has concluded that for each of them some critical security problems remain. Our strong assumption is that the problem of identities and of support algorithms must be addressed simultaneously. Another aspect is to clearly present to each node to the potential user rights and duties that he must observe when entering the network. Trust towards the implemented mechanisms could only be gained by enforcing that all nodes execute them without any modification or tampering. Nevertheless, such promising ideas have also been proposed both for ensuring the security of the identities and that of the algorithms supporting the network. Our approach combines some concepts similar to the best proposed in the two domains of our analysis. We have proposed to develop them in our framework to secure the MANET for a real use: MADNESS [36]. The immediate perspectives of our work will be to propose a prototype implementing our ideas to allow users to leave the world of "the impossible use of MANET" to a better world where they will be able to use them in a successful and flexible manner to work efficiently together.

DRAFT VERSION

REFERENCES

[1] D. Johnson, C. Perkins, J. Arkko: Mobility Support in IPv6. draft-ietf-mobileip-ipv6-21.txt February 26, 2003.

[2] F. Kargl, S. Schlott, M. Weber: Identification in Ad hoc Networks. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) Track 9.

[3] Y. Frankel, P. Gemmell, P. D. MacKenzie, M. Yung: Proactive RSA. In Proceedings of Crypto' 97, 1997.

[4] Y. Frankel, P. D. MacKenzie, M. Yung: Adpative security for the additive-sharing based proactive RSA. In Proceedings of Public Key Cryptography 2001, 2001.

[5] T. Rabin: A simplified approach to threshold and proactive RSA. In Proceedings of Crypto' 98, 1998.

[6] V. Shoup: Practical Threshold Signatures. In Proceedings of EUROCRYPT'00, 2000.

[7] M. Narasimba, G. Tsudik, J. H. Yi: On the utility of distributed cryptography in P2P and MANets: the case of membership control. In Proceedings of IEEE International conference on network protocol (ICNP), november 2003

[2] A part of this work is supported by the french funding agency ANR in the framework of the SARAH project.

[8] N. Saxena, G. Tsudik, J. H. Yi: Admission control in Peer-to-Peer: Design and Performance evaluation. In ACM Workshop on Security of ad hoc and sensor networks (SASN), oct 2003

[9] L. Zhou, Z. J. Haas: Securing ad hoc networks. In IEEE Network Magazine, 13(6), November-December 1999.

[10] S. Yi, R. Kravets: MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks. The 2nd Annual PKI Research Workshop (PKI 03)

[11] H. Luo, S. Lu: Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks. Technical Report TR-2000.

[12] J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang: Providing robust and ubiquitous security support for mobile ad-hoc networks. In the Proceedings of the 9th International Conference on Network Protocols (ICNP'01), 2001.

[13] S. Micali: Efficient certificate revocation. MIT Laboratory for Computer Science, Tech. Rep. TM-542b, Mar. 1996.

[14] D. Boneh, M. Franklin: Identity-Based Encryption from the Weil Pairing. Lecture Notes in Computer Science, vol. 2139, pp. 213229, 2001.

[15] R. Hinden, S. Deering: IP Version 6 Addressing Architecture. Request for Comments 2373, July 1998. http://www.ietf.org/rfc/rfc2373.txt

[16] T. Aura: Cryptographically Generated Addresses (CGA). Request for Comments 3972, March 2005 http://www.rfc-editor.org/rfc/rfc3972.txt

[17] G. Montenegro, C. Castelluccia: Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses. Network and Distributed System Security Symposium (NDSS), Feb. 2002, http://citeseer.nj.nec.com/montenegro02statistically.html.

[18] S. Capkun, L. Buttyán, J.P. Hubaux: Small worlds in security systems: an analysis of the PGP certificate graph. In Proceedings of the 2002 workshop on New security paradigm: NSPW'02. Virginia Beach, Virginia, USA.

[19] A. Tastinger: Privacy Digest: Books : PGP : Pretty Good Privacy

[20] J.P. Hubaux, L. Buttyán, S. Capkun: The Quest for Security in Mobile Ad Hoc Networks. In Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing 2001 (MobiHOC 2001), Long Beach, CA, USA

[21] S. Capkun, L. Buttyán, J.P. Hubaux: Self-Organized Public-Key Management for Mobile Ad Hoc Networks. Swiss Federal Institute of Technology Lausanne (EPFL), Tech. Report (Jun 2002)

[22] K. Fokine: Key management in Ad Hoc Networks. Master Thesis. September,2002. http://www.ep.liu.se/exjobb/isy/2002/3322/exjobb.pdf

[23] S. Capkun, J.P. Hubaux, L. Buttyán: Mobility helps security in ad hoc networks. In Proceeding of the 4th ACM international symposium on Mobile ad hoc networking & computing http://www.sigmobile.org/mobihoc/2003/papers/p46-capkun.pdf

[24] S. Gokhale, P. Dasgupta: Distributed authentication for peer-to-peer networks. Applications and the Internet Workshops, 2003.

[25] E. Atallah, S. Chaumette: A Smart Card Based Distributed Identity Management Infrastructure for Mobile Ad hoc Networks. In the proceedings of the First IFIP TC6 / WG 8.8 / WG 11.2 International Workshop, WISTP 2007: Worshop in Information Security Theory and Practices, Smart Cards, Mobile and Ubiquitous Computing Systems. Heraklion, Crete, Greece, May 9-11, 2007.

[26] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E. M. Belding-Royer: A Secure Routing Protocol for Ad Hoc Networks. In Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP). November 2002

[27] P. Papadimitratos, Z. J. Haas: Secure Routing for Mobile Ad hoc Networks. In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002).

[28] Y. Hu, A. Perrig, D. B. Johnson: Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. MobiCom'02, September 2326, 2002, Atlanta, Georgia, USA.

[29] Y. C. Hu, A. Perrig, D. B. Johnson: Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. In Proceedings of the ACM Workshop on Wireless Security (WiSe), pages 30-40, ACM, San Diego, CA, September 2003.

[30] S. Zhong, J. Chen, Yang Richard Yang: Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In Proceedings of IEEE Infocom '03, San Francisco, CA, April 2003.

[31] S. Marti, T.J. Giuli, K. Lai, M. Baker: Mitigating routing misbehavior in mobile ad hoc networks. In the proceedings of the 6th annual ACM/IEEE international conference on Mobile Computing and Networking (MobiCom'00), pp. 255-265, 2000.

[32] P. Michiardi, R. Molva: CORE: A COllaborative REputation mechanism to enforce node cooperation in mobile ad-hoc networks. In proceedings of the CMS '02: Communication and Multimedia Security Conference, August 2002.

[33] S. Buchegger, J. Y. Le Boudec: Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad-hoc networks. In Proceedings of 10th Euromicro PDP (Parellel, Distributed and Network-based Processing), pp. 403-410, January 2002.

[34] The Terminodes project: http://www.terminodes.org/

[35] L. Buttyán, J.P. Hubaux: Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks. Technical report, Swiss Federal Institute of Technology Lausanne, 2001.

[36] E. Atallah, P-F. Bonnefoi, C. Burgod, D. Sauveron: Mobile AD hoc Network with Embedded Secure System. AmI.d 2006. 20-22 septembre 2006, Nice, France.

DRAFT VERSION

Pierre-François Bonnefoi is Assistant Professor at the XLIM Laboratory (UMR CNRS 6172) of the University of Limoges (France). He obtained his Ph.D at the University of Limoges (France) in June 1999 and since january 2004 he is the leader of the Security of Information team. Since december 2005, Pierre-Franois is responsible for Limoges of the SARAH (Services distribus Asynchrones pour Réseaux Ad Hoc / Delay-Tolerant Distributed Services for Mobile Ad Hoc Networks) project. This project funded by the ANR (Agence Nationale pour la Recherche / National Agency for the Research) involves the LaBRI (Bordeaux, France), LIH (Le Havre, France), VALORIA (Vannes, France) and XLIM (Limoges, France) laboratories. His favourite research interests are Computer Science, Network and Security. More information on: `http://ishtar.msi.unilim.fr/`

Damien Sauveron is Assistant Professor at the XLIM Laboratory (UMR CNRS 6172) of the University of Limoges (France). He is member of: IFIP WG 8.8 Smart Cards, IFIP WG 11.2 Small System Security, IEEE, IEEE Broadcast Technology Society, IEEE Communications Society, IEEE Computer Society, IEEE Systems, Man, and Cybernetics Society, IEEE Vehicular Technology Society, IEEE Standards Working Groups, GT 3.7: "Sécurité des Systèmes d'Information" of the GDR I3 (a french national research group). From 01/02/2006 to 31/03/2006, I was invited researcher at the ISG-SCC (Information Security Group - Smart Card Centre) of the Royal Holloway, University of London (RHUL). Then, from the 01/04/2006 to 10/08/2006 I was in a postdoctoral position at the ISG-SCC of the RHUL. From 03/09/2001 to 02/09/2004, he worked during three years for the ITSEF of SERMA Technologies on the Java Card security. He obtained his Ph.D at the University Bordeaux 1 (France) in December 2004. During his thesis that he carried out in the Distributed Systems and Objects team of the LaBRI he was one of the main developers of a Java Card emulator, he introduced the concept of pre-persistance in Java Card and he highlighted a new category of attacks on the open multiapplication smart cards. More information on: `http://damien.sauveron.free.fr/`

Dr. Jong Hyuk Park received his Ph.D. degree in Graduate School of Information Security from Korea University, Korea. He is now a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He has been served as Chairs, Program Committee or Organizing Committee for many international conferences and workshops. He is the managing editor of the International Journal of Smart Home (IJSH) and Associate Editor of Security and Communication Networks (SCN). He has been served as a Guest Editor for international journals by some publishers: Oxford, Emerald, Hindawi, Springer, Elsevier, Inderscience, SERSC. His research interests include Digital Forensics, Security, Ubiquitous and Pervasive Computing, Context Awareness, Multimedia Service, etc. More information on: `http://parkjonghyuk.wo.ro/`

DRAFT VERSION