Access Control Mechanism for Mobile Ad hoc Network of Networks (MANoN)

Ali Al-Bayatti, Hussein Zedan, François Siewe
Software Technology Research Laboratory
De Montfort University
Leicester, UK
alihmohd@dmu.ac.uk, zedan@dmu.ac.uk, fsiewe@dmu.ac.uk

***Abstract*—Many military research efforts have concentrated on how to allow war-fighters to take advantage of all available information within the battlefield in a rapid and flexible manner. As a result, the development of the Global Information Grid (GIG) was the key enabler for this process; hence, adding to the development of the mobile networking part of the GIG, the concept of the Mobile Ad hoc Network of Networks (MANoN) is introduced. This paper proposes a novel access control mechanism achieving the prevention essential; defined in the ITU-T M.3400 security management recommendation to manage securely the future of military Network-Centric Warfare (NCW). The authors will employ formal description as a method of handling both sequential and parallel composition in flexible timely constrains, in addition, this technique will be evaluated using the Network Simulator (NS-2) to provide and check whether access control requirements are met in a comprehensive manner.**

***Keywords*-Mobile Ad hoc Network (MANET); Mobile Ad hoc Network of Networks (MANoN); Access Control; Formal Methods; Global Information Grid (GIG); Network-Centric Warfare (NCW)**

I. Introduction

In the early part of the 21^{st} century, the focus of many military research efforts was on how to allow war-fighters to take advantage of all available information within the battlefield in a rapid and flexible manner. As a result, the development of the Global Information Grid (GIG) was the key enabler of this process [1]. GIG is a United States (US) Department of Defense (DoD) communication project; its target is to provide agile, responsive, robust and global networking forces, sensors, users, platforms, and applications, which are used as a first step to accomplish Network-Centric Warfare (NCW) operations. NCW is a new military doctrine that seeks to translate information advantage into a competitive war-fighting advantage through the robust networking of forces distributed in large-scale conflict areas [2]. In order to add to the development of the mobile networking part of the GIG, we introduced the concept of MANoN [3]. MANoNs have various defining characteristics that differentiate them from other wired, wireless and even other ad hoc networks. MANoN is a combination of both the Mobile Ad hoc Network (MANET) [4] and a Network of Networks (NoN) [5], which are several nodes interconnected by wireless connections in a dynamic topology that lacks any infrastructure. Basically, each node is an ad hoc network in itself, with its own management and rules. In addition, MANoNs have the capability of operating under partial information, which makes them more flexible yet more configurable (evolvable) over time to networks joining and disconnecting, without affecting the main system. Figure 1 shows an idea of the GIG, consisting of different MANETs from different backgrounds and resources communicating with each other [5]. These unique characteristics will raise non-trivial challenges for MANoNs, such as security, routing, scalability, availability, deployment considerations, media access, and Quality of Service (QoS) [6] [7], in addition to conflicts which might occur because of conflicting policies (e.g. nodes following their own network policies and at the same time obeying different policies the new MANoN system might enforce adopted by different entities in the MANoNs.

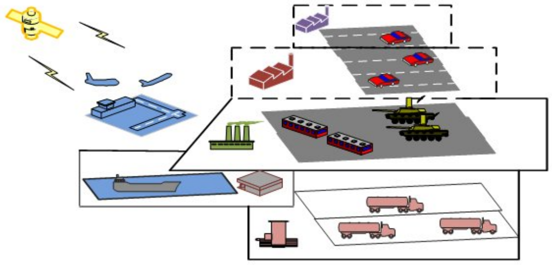


Figure 1. Global Information Grid (GIG)

In this paper, we propose an efficient access control mechanism based upon threshold cryptography digital certificates described by formal methods and evaluated using Network Simulator (NS-2) to highlight prevention against malicious nodes trying to bring the system down. The reminder of this paper will be organised as follows: Section II will present our security management System. Section III will describe our MANoN scenario. Section IV will explain our security architecture and its components. Section V will illustrate the implementation of our access control mechanism for MANoN. Section VI will describe the simulation results,

978-0-7695-3969-0/10 $26.00 © 2010 IEEE
DOI 10.1109/ICNS.2010.50

and finally, in Section VII we conclude our paper.

II. Security Management

Providing security management is critical for any system, and our MANoN is not exceptional; our security management will be described upon the recommendation ITU-T M.3400 [8] perspective, showing the three essential components:

- Security Administration
- Prevention and Detection
- Containment and Recovery

In any system, providing one of those components is a problem, but if we are dealing with an infrastructure-less MANoN, it will be a dilemma, yet we approached each set group independently, providing unusual solutions for each one of them. In this paper we will focus on providing prevention function sets, which are those needed to prevent intrusions. So, in order to prevent illegitimate users, access control requirements must be defined and satisfied; therefore, we designed novel *Access Control Mechanism* to satisfy these requirements. Section V explains our prevention mechanism, which is based on *authentication* and *authorisation* digital certificates in a pre-defined MANoN scenario.

III. Mobile Ad hoc Network of Networks (MANoN) Scenario

To aid the application of MANoN in any wireless environment, when required, and to achieve the services demanded by the user, we need to define MANoN as a whole object with clear syntax and semantics. In this section, we will present a framework scenario that can be applied to MANoN in different network environments, for example cellular systems, smart homes or military operations. Figure 2 depicts four MANETs; each network is a legacy under its own management and policies coming together to create a MANoN; each MANET has the ability to perform separately which enables it to disconnect and join without affecting the main MANoN system.

Networks 1, 2 and 4 are pre-defined and connected to exchange PKI information (Public keys P, Private keys Pr), whereas the undefined network is obviously not. Nodes in each MANET are classified into:

General Nodes (GN) are regular ground nodes which are typically soldiers equipped with communication and computation limited devices.

Back-Bone Nodes (BBN) are usually special units, such as tanks and personnel carriers, which have more extensive facilities than regular ground nodes. BBN nodes will carryout CAs (Servers CA$_{SE}$ and Combiners CA$_{C}$) duty [9].

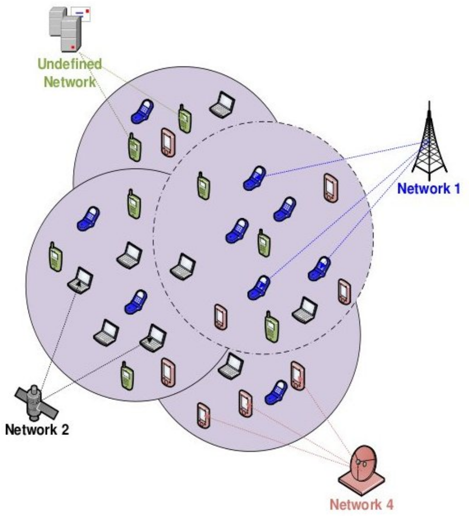


Figure 2. MANoN Scenario

It is relatively uncommon to have one node that belongs to more than one PKI, because this protocol is used either in civilian environments or military environments where the number of PKIs within a given area is limited. Before engaging into the MANoN, nodes in each MANET will receive from their MANET digital certificates (authentication and authorisation) that are based on the ITU-T recommendation X.509 [10] with the aim of operating in the MANoN. Authentication certificates will be used as identification (e.g. passport), whereas authorisation certificates will be used as security clearance, enabling nodes to operate with distinctive permissions. With the purpose of illustrating access control; special solutions and mechanisms must be applied. Thus, as a foundation to our system, first we build security architecture to provide an end-to-end security solution based on the ITU-T recommendations: X.800 and X.805 [11] [12]. Second, we present digital certificates of the prevention technique which will provide Access control mechanism for MANoN nodes, achieving the set of security requirements any system might need to survive: Authentication, Authorisation.

IV. Security Architecture

As we have learned from the history of security attacks [13], security cannot be considered separately after the whole system of networks has been designed; rather, security must be considered as an inseparable aspect of the development of the network. As a result, this security architecture was created to address the global security challenges of consumers, users, services and other applications, in order to prevent any type of attacks, external or internal, passive or active. Our Security Architecture can be found in [3].

V. Implementation of Access Control Mechanism for MANoN (ACM-MANoN)

Various technologies can be used to satisfy the access control requirement defined in [3]. Modern cryptography [14] – including public key cryptography, digital signatures and digital certificates – are the most powerful tools that can be used to implement most security requirements, including authentication, authorisation, data confidentiality, data integrity and non-repudiation. The unique characteristics of MANoN make the application of these technologies a real challenge. In this paper, this issue is tackled by proposing new security mechanism, the access control mechanism. The proposed security mechanism will focus on the proceeds of the trust infrastructure and application layers defined in [3]. This is because of the importance of this object in representing the main functionalities of MANoN as a wireless access networks.

As shown, the security mechanisms will satisfy authentication, authorisation and help toward forcing other security requirements such as availability, data confidentiality, data integrity and non-repudiation. As mentioned, all nodes receive their keys and certificates (authentication, authorisation) from their PKI (MANET); moreover, the MANoN service has its own P/Pr keys; all BBN (Servers CA$_{SE}$, Combiners CA$_{C}$) will receive a share of the Pr (sign certificates and perform threshold cryptography [9]) and the P in order for CA$_{C}$ to validate other MANoN certificates. So, for example, if $node\ x$ from network 1 (Network (1) defined in our MANoN) is trying to engage into our MANoN system, $node\ x$ will broadcast his request for an authorisation certificate (perform in network (2) MANoN) attached with his own authorisation and authentication certificates that he has received from his original network. After receiving the request from $node\ x$, the CA$_{C}$ in the correspondent network will validate the certificates by using the service public-key P$_{PKI1}$ to which $node\ x$ belongs. If the certificates are valid, the CA$_{C}$ tries to find set of $(t+1)$ correct partial signatures to generate digital signature by the CA$_{SE}$ (performing threshold cryptography) in order to create an authorisation certificate with a specific degree of security clearance, depending on the security clearance (Certificate Policies) $node\ x$ certificate carries. After creating the authorisation certificate, the combiner will forward the certificate to the new node with the intention of using it in the correspondent network.

The following variables represent the parameters of the ACM-MANoN:

- n: number of networks in the MANoN; networks are numbered from 1 to n;
- n_i: number of nodes, including certificates authorities, in the network i, $1 \leq i \leq n$; nodes in a network i are numbered from 1 to n_i;
- t_i: number of certificate authority server in the network i, $1 \leq i \leq n$;
- CAS_{ij}: certificate authority server j of the network i, for $1 \leq j \leq t_i$ and $1 \leq i \leq n$;
- CAC_i: certificate authority combiner j of the network i, for $1 \leq i \leq n$;
- DC_{xij}: authentication digital certificate of the node j in the network i, for $1 \leq j \leq n_i$ and $1 \leq i \leq n$;
- DC_{yij}: authorisation digital certificate of the node j in the network i, for $1 \leq j \leq n_i$ and $1 \leq i \leq n$;
- Pb_{ij}: publick key of the node j in the network i, for $1 \leq j \leq n_i$ and $1 \leq i \leq n$
- Pr_{ij}: private key of the node j in the network i, for $1 \leq j \leq n_i$ and $1 \leq i \leq n$
- Pk_i: public key of network i, $1 \leq i \leq n$
- S_{ij}: share of the certificate authority j of the private key of network i, for $1 \leq j \leq t_i$ and $1 \leq i \leq n$;

Before defining our access control mechanism, conditions of healthiness for the variable above must be defined.

- $Pb_{ij} \neq Pb_{uv}$ for $i \neq u$ or $j \neq v$
- $Pr_i \neq Pr_j$ for $i \neq j$
- $Pk_i \neq Pk_j$ for $i \neq j$

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

1) Granting certificate authority duties to nodes:

$$\forall i, j.(1 \leq j \leq n_i) \wedge (1 \leq j \leq n) \wedge (CAS_{ij} = t_i) \\ \wedge (CAC_i = t_i + 1)$$

Here we choose the high ranked t_i nodes of each network i to play each the role of *Certificate Authority Server* and the node $t_i + 1$ to be the *Certificate Authority Combiner*, for the network i.

2) Issuing digital certificates to local nodes of each network:

$$\forall i, j.\big((1 \leq j \leq n_i) \wedge (1 \leq j \leq n) \wedge (DC_{xij} =< j, i, \\ sdx_{ij}, edx_{ij}, CAC_i, Pb_{ij}, \ldots, Sigx_{ij} >) \wedge \\ (DC_{yij} =< j, i, sdy_{ij}, edy_{ij}, CAC_i, \\ PB_{ij}, c_{ij}, \ldots, Sigy_{ij} >).\big)$$

where c_{ij} is the security clearance of the node j in the network i; sdx_{ij} and edx_{ij} are the start and end date of the authentication digital certificate; sdy_{ij} and edy_{ij} are the start and end date of the authorisation digital certificate; and the digital signature of the certificates $Sigx_{ij}$ and $Sigy_{ij}$ are calculated by the certificate authority combiner CAS_i of the network i by performing a threshold cryptography involving the certificate authority servers CAS_{iv} and their shares S_{iv} of the private key of the network i, for $1 \leq v \leq t_i$.

Each node uses its digital certificates (authentication and authorisation) to request services within the network to which it belongs. However, in order to access services in an external network, a node needs to request from that network a new authorisation certificate in order to perform in it.

3) A request for digital certificates from a node j of the network i to an external network can be modelled by a message of the form: $< j, i, X, Y >$ for some authentication digital certificate X and some authorisation certificate Y.

4) Such a request $< j, i, X, Y >$ is checked by the external networks CA combiner as follows:

   a) The requester is the owner of the authentication and authorisation certificates, i.e.
   $(X^1 = j) \wedge (Y^1 = j)$;

   b) The network of the requester is the network where the digital certificates X and Y were issued, i.e.
   $(X^2 = i) \wedge (Y^2 = i)$;

   c) The digital certificates have not expired, i.e.
   $(X^3 \leq today \leq X^4 \wedge (Y^3 \leq today \leq Y^4)$;
   Where today denotes the current date;

   d) The digital certificates X and Y are authenticated using the public key Pk_i of the network i and a signature verification algorithm for threshold cryptography.

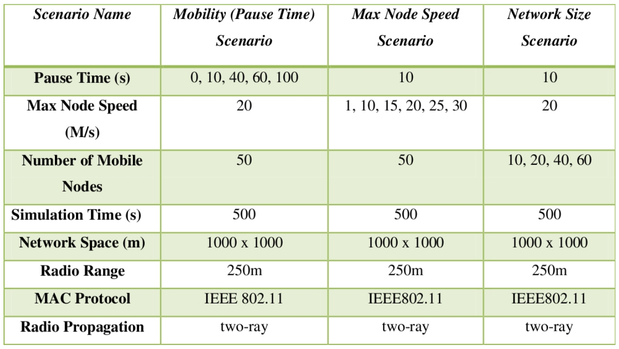
5) Issuing digital certificates to an external node j of the network i for it to access services in the network k, $k \neq i$. Here, we suppose that the corresponding request has been successfully authenticated and verified as per step 4 above. The node j of the network i will be issued a new authentication $exDC_{xkj}$ and authorisation $exDC_{ykj}$ digital certificates as follows:

$$exDC_{xkj} =$$
$$< j, i, sdx_{ji}, edx_{ij}, CAC_k, \ldots, exSig_{xkj} >$$
$$exDC_{ykj} =$$
$$< j, i, sdy_{ij}, edy_{ij}, CAC_k, c_{kij}, k, \ldots, exSig_{ykj} >$$

Where c_{kij} is the security clearance of the node j of the network i in the external network k; and digital certificate of the certificates $exSigx_{kj}$ and $exSigy_{kj}$ are calculated by the certificate authority combiner CAC_k of the network k by performing a threshold cryptography involving the certificate authority servers CAS_{kv} and their shares S_{kv} of the private key of network k, for $1 \leq v \leq t_k$.

VI. Simulation Results

This section will show the results of providing Authentication and Authorization certificates to the nodes of our MANoN system. NS-2 simulations have been carried out to evaluate the performance of the proposed scheme in the pre-defined scenario. The parameters used for simulation are depicted in Figure 3.



Scenario Name	*Mobility (Pause Time) Scenario*	*Max Node Speed Scenario*	*Network Size Scenario*
Pause Time (s)	0, 10, 40, 60, 100	10	10
Max Node Speed (M/s)	20	1, 10, 15, 20, 25, 30	20
Number of Mobile Nodes	50	50	10, 20, 40, 60
Simulation Time (s)	500	500	500
Network Space (m)	1000 x 1000	1000 x 1000	1000 x 1000
Radio Range	250m	250m	250m
MAC Protocol	IEEE 802.11	IEEE802.11	IEEE802.11
Radio Propagation	two-ray	two-ray	two-ray

Figure 3. NS-2 Simulator Parameters

It can be argued, that the success ratio is one of the most significant factors that measure the number of successful certificate authentication and authorisation requests to the total number of certificate authentication requests that take place during the simulation time. As an assumption, each node will make at least one authentication request. Therefore, the total number of authentication requests made during the simulation time is equal to the number of nodes trying to enter the MANET. Figure 4 shows the success ratio against mobility and network size. Mobility is most often a big issue in developing ad hoc protocols. As can be seen, our MANoN is not much affected by mobility. In general, the success ratio increases with high mobility situations and large network sizes. The effect of mobility is more noticeable with a small number of nodes. This is because of the number of neighbour nodes. The number of neighbour nodes based on transmission range and simulation area can be calculated using the following formula [15]:

$$\frac{(\pi \times r^2)}{[\frac{w \times h}{n}]}$$

Where w = area width, h = area height, r = transmission range, n = number of nodes. For example, when the network size is 10, the number of neighbours is around 1.96, but when the network size is 30 the number of neighbours is more than 6. Therefore, the effect of mobility increases with a smaller number of nodes, because high mobility reduces the effect of fewer neighbourhoods.

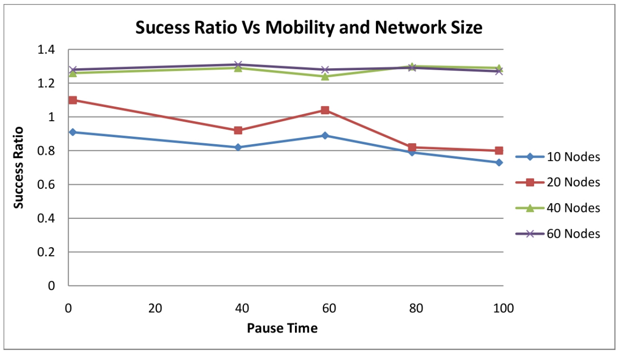


Figure 4. Success Ratio Versus Mobility and Network Size

Similarly to success ratio, overhead is considered essential to any system. Overhead is the number of packets generated by this security protocol. There are three types of packets in our MANoN algorithm: certificate packets, request packets and reply packets. For a MANoN with N nodes, the total number of generated packets is equal to the number of certificate packets, the number of request packets $(Max(N))$ and the number of reply packets $(Max(N))$. This explains why the overhead is almost unchanged for the same number of nodes. The overhead has been calculated against mobility and network size. This explains why the overhead is almost unchanged for the same number of nodes. As mobility decreases, the overhead increases slightly, especially when the network size is greater than 10 nodes, as depicted in Figure 5 . It is also obvious from this figure that the overhead increases with an increase in network size.

VII. Conclusion

In this paper, we have dealt with the mobile part of the Global Information Grid (GIG) known as Mobile Ad hoc Network of Networks (MANoN). We have focused on providing the prevention security essential, based upon digital certificates threshold cryptography expressed by formal description methods and evaluated using Network Simulator (NS-2). We expect that this security solution could be used to satisfy security for any wireless systems that have the same properties as our system.

Acknowledgment

Ali Al-Bayatti would like to thank Mohammed Al-Sammarraie for his support in LaTeX, cheers mate.

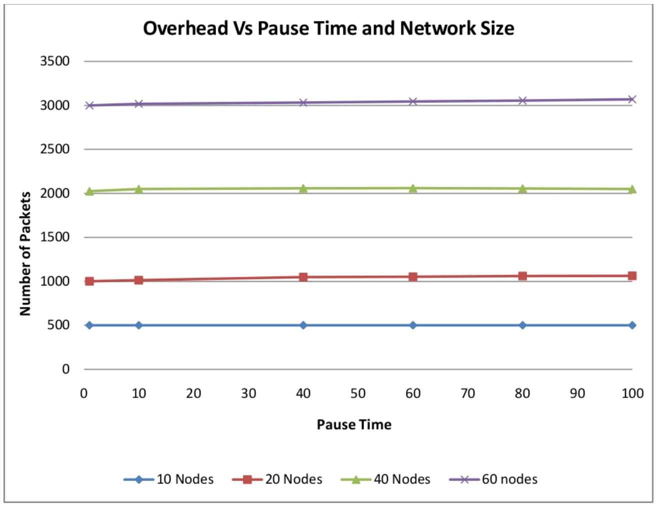


Figure 5. Overhead Versus Mobility and Network Size

References

[1] L. Stotts, S. Seidel, T. Krout, and P. Kolodzy, "Manet gateways: radio interoperability via the internet, not the radio," *Communications Magazine, IEEE*, vol. 46, pp. 51–59, June 2008.

[2] J. Predd, S. L. Pfleeger, J. Hunker, and C. Bulford, "Insiders behaving badly," *IEEE Security and Privacy*, vol. 6, no. 4, pp. 66–70, 2008.

[3] A. H. Al-Bayatti, H. Zedan, and A. Cau, "Security solution for mobile ad hoc network of networks (manon)," in *ICNS '09: Proceedings of the 2009 Fifth International Conference on Networking and Services*, (Washington, DC, USA), pp. 255–262, IEEE Computer Society, 2009.

[4] C. K. Toh, *Ad Hoc Wireless Networks: Protocols and Systems*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

[5] B. Spencer and J. Ironside, "Network centric warfare operation in an expeditionary context," *Symposium of South Africa, MICSSA, Military Information Communications*, pp. 1–12, 2007.

[6] C. S. R. Murthy and B. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2004.

[7] M. Ilyas and R. C. Dorf, eds., *The handbook of ad hoc wireless networks*. Boca Raton, FL, USA: CRC Press, Inc., 2003.

[8] I. T. U.-T. Recommendation(M.3400), "Telecommunication management network (tmn)," 2000.

[9] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, pp. 24–30, 1999.

[10] I. T. U.-T. Recommendation(X.509), "Public-key and attribute certificate frameworks," 2005.

[11] I. T. U.-T. Recommendation(X.800), “Security architecture for open systems interconnection for ccitt applications,” 1991.

[12] I. T. U.-T. Recommendation(X.805), “Security architecture for systems providing end-to-end communications,” 2003.

[13] P. Chandra, *BULLETPROOF WIRELESS SECURITY: GSM, UMTS, 802.11, and Ad Hoc Security (Communications Engineering)*. Newnes, 2005.

[14] W. Stallings, *Cryptography and Network Security (4th Edition)*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 2005.

[15] S. Kurkowski, T. Camp, and M. Colagrosso, “Manet simulation studies: The incredibles,” *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9, pp. 50–61, 2005.