Security Applications for Ad Hoc Networks

Antônio Carlos Castañon Vieira[1,2], Sergio Luiz Cardoso Salomão[1], Aloysio de Castro Pinto Pedrosa[2], Antônio Carneiro de Mesquita Filho[2]

[1] Information Technology Department Brazilian Army Research and Development Institute – IPD Av. Das Américas 28705, 23020-470, Rio de Janeiro, RJ Brazil – Brazil

[2]Department of Electrical Engeneering COPPE/Federal University of Rio de Janeiro
P.O. Box 68504 21945-970 Rio de janeiro, RJ, Brazil University

{castanon, salomao, mesquita}@lpc.ufrj.br), aloysio@gta.ufrj.br

Abstract. *Nowadays, data security is an important issue in telecommunication network to be considered in its implementation and operation, mainly in wireless network without infrastructure as the Ad Hoc networks. This paper presents the Godzuk symmetric cryptographic algorithm, as a possible standard for this kind of mobile communication.*

Resumo. *Atualmente, segurança das informações é uma importante característica a ser considerada nos projetos e operações das redes de telecomunicações, sobretudo, nas redes sem fio e sem infra-estrutura como as redes Ad Hoc. Este artigo descreve o algoritmo criptográfico simétrico Godzuk, como um possível padrão para este tipo de comunicações móveis.*

1. Introduction

Telecommunication networks, where organizations are often located in remote areas, where terrestrial infrastructure is not in place or damaged by disaster, making impossible to have base stations. An ad hoc network is the most suitable due to be a collection of wireless nodes that do not need to rely on a predefined infrastructure to keep the network connected.

In the last years, the wireless networks are being increasingly deployed for military applications, especially in the battlefields where a networks needs to be formed very fast on an ad hoc basis without the support of any fixed infrastructure.

In this way, security stands out as a critical issue in the design of such networks. This has been necessitated by the fact that free-space radio transmission in wireless networks makes eavesdropping easy and consequently, a security breach may result in unauthorized access, information theft, interference, jamming and service degradation. What makes it worse is that the sender and the intended receiver have little means of knowing whether the transmission has been intercepted or not, so the intrusion is virtually undetectable. While security for wireline networks have matured in both research and commercial environments, the design and deployment of security in wireless networks is relatively still an evolving field. Thus, the overall understanding of security solutions for wireless networks will be of tremendous importance and significance not only to the research community but also to the wireless industry community[2].

The Godzuk´s hardware implementation is suited as Ad Hoc standard for two main reasons. The first one is its high performance on cipher and decipher data operations, since all information used on mobile network have to be protected with cryptography, needing a algorithm faster than 1Mbits/s, that is some radio specifications for mobile applications[6]. The second one is the circuit size required for this application. Many others symmetric cryptographic algorithms are faster than those [3,4]. However, for archiving such rate, they need more area. GODZUK is a possible solution for this problem.

This work is organized in six sections. Section 2 shows the basic idea about Ad Hoc Networks. Section 3 describes the security method used in Ad Hoc Networks. Section. Section 4 states the GODZUK cryptographic algorithm. Section 5 shows the performance of this algorithm. Finally, section 6 presents the conclusions.

2. AD HOC NETWORK

Ad Hoc networks are a new paradigm of wireless communication for mobile host. In this kind of network, there is no fixed infrastructure such as base stations as in mobile telephone or mobile switching centers as in trunk communications.

Each node acts a router transmitting messages from one node to another. These nodes also need to perform all other functions involved in any network.

One of the most important features in Ad Hoc network is its mobility, which causes frequent changes of the network topology, making it very difficult to incorporate many network controls.

Figure 1a shows such an example: initially, node A and D have a direct radio link between them. When D moves out of A's radio range, as showed in figure 1b, the link is broken. However, the network is still connected, because A can reach D through C, E and F.

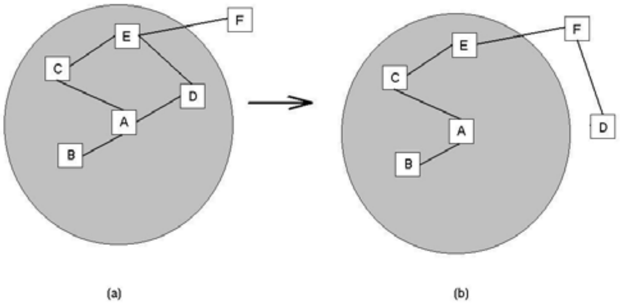

Figure 1: Topology changed in Ad Hoc networks.

As can be seen from above, the Ad Hoc network is quite different from traditional network. In [7, 8], salient feature of the Ad Hoc networks are analyzed as the following: Dynamic topologies; Bandwidth-constrained, variable capacity links; Energy-constrained operation and Wireless vulnerabilities and Limited physical security.

Operation in an ad hoc network introduces some new security problems in addition to the ones already present in fixed networks. Mobile wireless networks are generally more prone to physical security threats. The possibility of eavesdropping, spoofing, denial-of-service, and impersonation attacks is increased. Existing link security techniques are often applied within wireless networks to reduce security threats.

3. Security in AD HOC NETWORKS

Wireless networks are more prone to security attacks as all transmissions are carried out using the air medium. They are especially susceptible to attacks of eavesdropping, replay and spoofing. These systems therefore need to have built-in features to withstand these attacks without compromising security in any way [2].

The classification of security services in any network can be given as follows [12]: Confidentiality, Encryption, Integrity, Access Control and Availability.

Existing solutions for the security of wired networks could be applied to wireless environments. Nevertheless, the intrinsic characteristics of wireless networks (absence of centralized infrastructure, mobility of the nodes, limited bandwidth, etc) may limit their application. For instance, key certification as implemented in a public key infrastructure usually relies on a point of centralization (CA). Such centralized architectures are not adapted to the dynamic topology of MANETS. In such networks, the mechanisms implementing continuous services, such as security functions, should be distributed.

3.1 Group Key establishment

According to the security goals to be achieved, several mechanisms can be implemented on different network layers. Most existing mechanisms are based on cryptography and certification must be implemented to secure key exchanges. However they need a strong way to change secret key.

In [5], they showed many ways to manage group key, includes activities for establishment, maintenance and distribution of the group key. Maintenance activities consist of changing the group key due to group members addition or exclusion or due to the use of the group key for long periods of time (key refresh). A good key management policy is extremely important for the deployment of security services. The group key establishment can be centralized, also called distributive, where an entity is responsible for generating the group key and distributing it to the other group members. This approach has the advantage of being simple. In a distributed, or contributory, key establishment all group members contribute for the group key generation. This approach is fault tolerant and diminishes the risks of vicious key generation by a single entity.

It was defined that the CLIQUES protocol suite [18] was considered a good alternative for Ad Hoc environments due to its high performance in respect to the number of message and to the number of operations required, as well as, there is no need for synchronism among the group member sequence to take place during the group key establishment .

Based in this previous work [5], we present, therefore, a symmetric cryptographic algorithms, Godzuk, implement in hardware, as a possible standard for Ad Hoc network, in order to archive the security needs of this kind of network.

4. ALGORITHM PROPOSED for Security in AD HOC NETWORKS

In this section we will present cryptographic algorithm, select to this application. It is symmetric and based in Feistel network [10], it is considered unbroken and not patented. Those features and the fact of its high performance in hardware, were decided to choose then as a possible standard for Ad Hoc Network.

In terms of cryptanalysis, it is strong enough for this kind of applications [10]. It has strength of a cipher against linear and differential cryptanalysis by two security parameters - “linear” probability [13] and “differential” probability [14].

4.1 – GODZUK cryptographic Algorithm

The cryptographic GODZUK algorithm is a version of the GODZILLA [9] algorithm, developed to be used in the third generation of cellular (according to the norms of the 3GPP).

As GODZILLA, GODZUK is an algorithm of symmetrical key, whose operation structure is based on Feistel Network [12]. The algorithm operates with blocks of 64 bits and with key of 128 bits, according to demands of the 3GPP. The algorithm is executed in eight rounds on Feistel Network. In the same way that in GODZILLA, the internal operations of the algorithm are operations of OR - exclusive, executed now in only two levels of functions SMER [16]. The Figure 2 shows the cipher operation for the GODZUK cryptographic algorithm, that is executed in eight rounds, with the following operation:

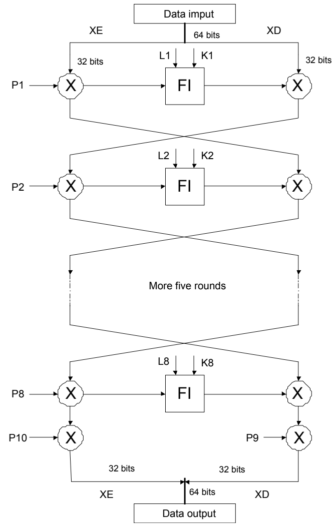

Figure 2: GODZUK cipher operations

```
    Divide the 64 bits input block in two sub-blocks of 32 bits, XE and XD;
    for i = 1 to 8 do:
    XE = XE XOR Pi;
    XD = FI(XE) XOR XD;
if the number of rounds is different from 8:
```

```
Exchange XE and XD;
else
Don't exchange XE and XD;
XE = XE XOR P10;
XD = XD XOR P9;
Combine XE and XD to obtain the cipher data of  64 bits.
```

The used sub-keys are: ten sub-keys Pi of 64 bits, eight sub-keys Li of 48 bits and 8 sub-keys Ki of 84 bits. The method for sub-keys generation can be found in [9].

Function FI

The function FI, it is also an algorithm of three rounds based on Feistel Network. The operation form is plenty similar to the FI's main block in GODZUK.

```
Divide the 32 bits input block in two sub-blocks of 16 bits, XE and XD;
for J = 1 to 3 do:
XE = XE XOR LI,J;
XD = FS(XE) XOR XD;
Combine XE and XD to obtain the cipher date of 32 bits.
```

The sub-keys used in the execution of each function FI are: three sub-keys Li,j of 16 bits, obtained by the division of each sub-key Li(48 bits) in three new sub-keys Li,j(16 bits); three sub-keys Ki,j of 28 bits, obtained by the division of the sub-key Ki(84 bits) in three new sub-keys Ki,j(28 bits).

Function FS: is a special function based on Scheduling by Multiple Edge Reversal techniques, Figure 4, it named SMER function [10]. This SMER function used has the following configuration:

- two nodes and fifteen edges.
- ri and rj are coprime numbers, making possible Nc (cycle number) be maximum, i.e., Nc = (ri + rj) / gcd(ri, rj) = 16.

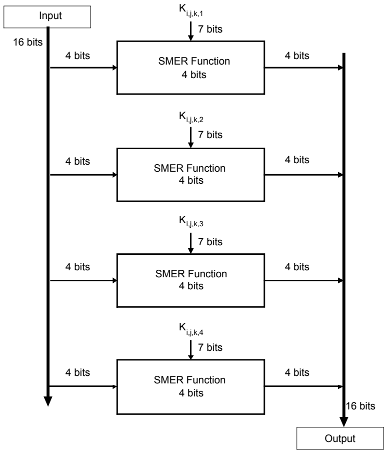

Figure 3: FS function based on SMER functions

The possible configurations of ri and rj that satisfy Nc=16 are shown in Table 1.

Table 1. Possibile Configurations of ri and rj.

Ri	Rj	Configuration
1	15	000
3	13	001
5	11	010
7	9	011
9	7	100
11	5	101
13	3	110
15	1	111

The ri and rj combination is called SMER configuration. Each SMER configuration has 16 states, depicted in Figure 4(a). The node is associated to 4 bits and these bits are the SMER function input, as shown in Figure 4(b). The SMER function input determines the initial state. The SMER key contains two parts, as shown in Figure 4(c). The configuration part, ``b7 b6 b5", represents the possible SMER configurations, i.e, determines the combination of ri and rj. The cycle number part, ``b4 b3 b2 b1", determines how many steps will be necessary in order to obtain the final state. This final state produces the four-bit output. More information can be found in [10].

As example, suppose that the SMER key is ``0010100". The bits ``001" determine the SMER configuration, therefore ri = 3 and rj = 13. The cycle number is supplied by the bits ``0100". Assigning ``1010" to the SMER input, we obtain the SMER output ``0110", as shown in Figure 6 (a). The process of retrieving data works on the same way, however the bits associated to cycle number need to be changed by its complement. In the above example, the new SMER key will be ``0011011". For this new key and the SMER input being ``0110", the SMER output will be ``1010",i.e., the same value that was apply on the first step of this example.

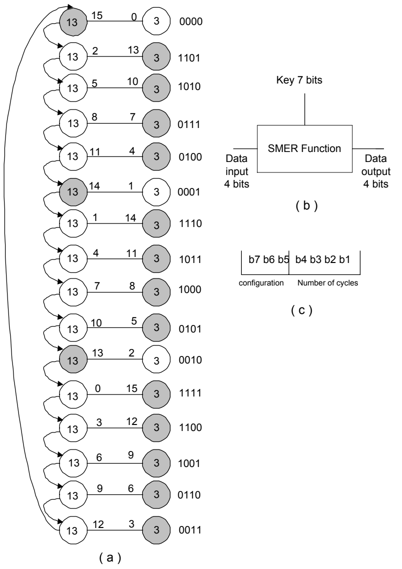

Figure 4: SMER Function

5. HARDWARE IMPLEMENTATIONS

5.1 – GODZUK

Initially, the GODZUK cryptographic algorithm was described in VHDL at the structural level resulting in the GODIZUK Soft-core. It can be used to synthesize hardware implementation of the GODZUK.

The soft-core was implemented also using a 0,7µm two metal CMOS technology. This implementation resulted in a clock frequency (typical case) of 78 MHz and in a ASIC core, from synopsys tools, equal to 9870 equivalent gates. The final encryption rate is about 255Mbits/s (or 3,26 Mbits/s to 5,000 data bits), which fully satisfies mobile communications rules [17].

Table 2. GODZUK and performances.

Algorithm	Equivalent gates	PC Pentium Througput	FPGA Througput	ASIC Throughput
GODZUK	9870	ND	56 Mbits/s (18MHz)	255Mbits/s (78MHz)

6. CONCLUSIONS

In this paper we analyzed some security solutions for Ad Hoc Network. We present a symmetric cryptographic algorithms – Godzuk. It is based on Feistel Network and it is considered unbroken and not patented. Thus, it has been showed as a good solution for mobile communications in Ad Hoc Network.

The difficulty to define a standard cryptographic algorithm to Ad Hoc Network resides in the compromise among security, complexity (measure in equivalent gates) and performance.

It was shown that, GODZUK is categorized as symmetric cipher algorithm. It operates with 64-bit data (cipher or decipher) and can operate with 128-bit secret-key, that can be feasible and safer change in unsafe channel with the CLIQUES protocol suite. They have provable security against differential cryptanalysis and linear cryptanalysis.

GODZUK can be used as an algorithm for authentication confidentiality and integrity in mobile systems. It is reasonably fast and small in hardware to attend requirements for Ad Hoc Network.

Our implementation of the GODZUK algorithm on the FPGA or ASIC demonstrated that it is possible to have a flexible, cheap and high performance implementation of a cryptographic algorithm on a standard host in Ad Hoc Network.

7. REFERENCES

[1] D. P. Agrawal, "Future directions in mobile computing and networking systems," Mobile Computing and Communications Review, Vol. Vol. 3, pp. 13-18, Oct 1999.

[2] Z. J. Haas,L. Zhou, " Securing ad hoc networks," IEEE Network Magazine, vol. Vol13, nov/dec 1999.

[3] Vieira, A.C.C. and Salomão, S. L. C. et al, "SCOB, A Soft-core for the Blowfish cryptographic algorithm" published in the proceedings of the XII Brazilian Symposium on Integrated Circuits, Oct 1999.

[4] Salomão, S.L.C. et al "Hipcrypto: A high-performance VLSI cryptographic chip", published in the proceedings of the 11th Annual IEEE International Asic Conference (ASIC98), September 1998.

[5] Anton, E. R. and Duarte, O. C. M. B. - "Group Key Establishment in Wireless Ad Hoc Networks", Workshop em Qualidade de Serviço e Mobilidade - WQoSM 2002, Angra dos Reis, RJ, Brazil, November 2002.

[6] Specification of the Bluetooth System, version 1.1 February 2001, Official Bluetooth Website <http://www.bluetooth.com/>.

[7] S. Corson, J. Macker: Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, 1999, <ftp://ftp.funet.fi/pub/standards/RFC/rfc2501.txt>

[8] S. Corson, J. Macker, G. Cirincione: Internet-based Mobile Ad Hoc Networking, published in the IEEE Internet Computing, Jul/Aug 1999.

[9] Barbosa, V., An Introduction to Distributed Algorithms. published in the MIT Press, 1996.

[10] Salomão, S.L.C., "Architectures in Hardware to Cryptographic Accelerators", Doctor Thesis, COPPE/UFRJ, Rio de Janeiro, Brazil, 2000.

[11] Salomão, S.L.C. et al, " Improved IDEA" published in the proceedings of the 13th Symposium on Integrated Circuits and System Design –-SBCCI 2000, September 2000, Brazil.

[12] Schneier, Bruce, "Applied Cryptography", Second Edition, John Wilwy & Sons inc., 1996.

[13] Nyberg, K.: "Linear Approximation of Block Ciphers", published in the Proceedings of Eurocrypt´94. Springer-Verlag 1995.

[14] Nyberg, K., Knudsen, L.: "Provable Security against Differential Cryptanalysis", published in the Journal of Cryptology, vol. 8, No.1, 1995.

[15] Salomão, S.L.C., et al. "Hardware Implementation of KASUMI Cryptographic Algorithm for Third Generation Mobile Systems", published in the 1st IEEE South-American Workshop on Circuits and Systems – SAWCAS´2000, nov, 2000, Brazil

[16] França, F.M.G. " Scheduling weightless systems with self-timed Boolean networks" published in the Workshop on Weightless Neural Network, April 1996.

[17] Vieira, A.C.C. and Salomão, S. L. C. et al, "Godzuk Cryptographic Algorithm for 3rd Generation Mobile Systems" published in the proceedings of the IEEE International Telecommunications Symposium -ITS2002, Sep 2002.

[18] M. Steiner, G. Tsudik e M. Waidner, "CLIQUES: A New Approach to Group Key Agreement", published in 18th International Conference on Distributed Computing Systems, may 1998.