*JKAU: Eng. Sci.,* **Vol. 21** No.2, pp: 3-14 (1431A.H./2010 A.D.)
DOI: 10.4197 / Eng. 21-2.1

# Simulation of IPSec Protocol in Ad-Hoc Networks

**A. A. Adas** and **T. A. Shawly**
*Department of Electrical and Computer Engineering, Faculty of Engineering, KAU, P.O.Box 80204, Jeddah 21589, Saudi Arabia*
*aadas@kau.edu.sa and tshawly@tvtc.gov.sa*

*Abstract.* This paper focuses on securing communication between nodes of ad-hoc networks by applying IPSec. Ad-hoc network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. The security factor is one of the main issues as no infrastructure-based solutions are applicable in this area. Like in all other networks, the routing is one of the most important parts in this network. Ad-Hoc On-demand Distance Vector (AODV) routing protocol is the most popular routing protocol in ad-hoc networks and it is employed in the simulation model. Security in ad-hoc network requires both routing security and data communication security. The proposed IPSec implementation model for both authentication header (AH) and encapsulation security payload (ESP) is simulated using the NS-2 simulator and results from the NS-2 simulated environment are compared for both authentication header and encapsulating security payload for secure data communication in ad-hoc networks. The main contribution of this paper is to present IPSec as a good solution for Ad-hoc network security problems.

## 1. Introduction

Since their emergence in the 1970s, wireless networks have become increasingly popular in the computing industry. This is particularly true within the past decade which has seen wireless networks being adapted to enable mobility. There are currently two variations of mobile wireless networks. The first is known as infrastructure networks, those networks with fixed and wired gateways. The bridges for these networks are known as base stations. A mobile unit within these networks

communicates with the nearest base station that is within its communication radius.

The second type of mobile wireless network is the infrastructureless mobile network, commonly known as an ad-hoc network. Ad-hoc networks have no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network, as shown in Fig. 1.

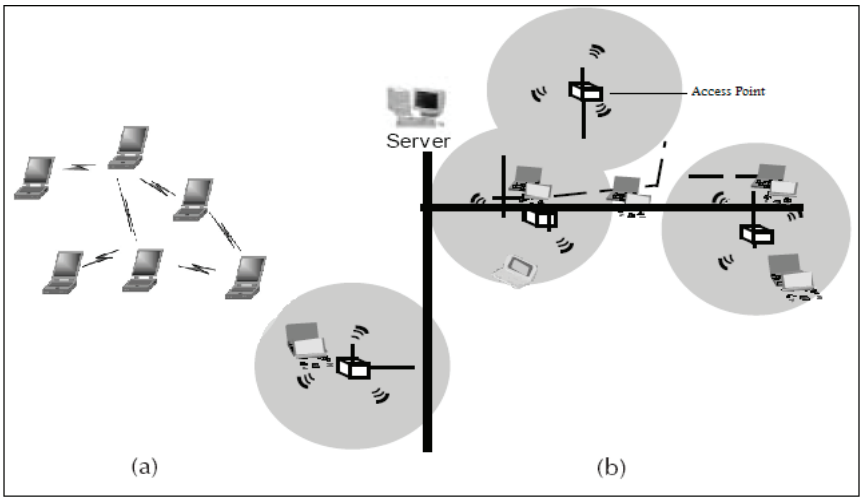


**Fig. 1. WLAN configurations: (a) Ad-hoc; (b) Infrastructure.**

In an ad-hoc network environment, much of the work is done to increase the security of the network. A good number of routing protocols have been proposed and used without ensuring proper security mechanism. As Ad-hoc On-Demand Distance-Vector (AODV) protocol is about to become a standard, researchers are now thinking highly about the security of this routing protocol. Besides, for ensuring security of an ad-hoc wireless network, a set of challenges are facing the researchers such as [1]:

- Dynamic topologies without central authority
- Bandwidth constraint
- Limited resources
- Secure data communication

Most of the security threats and vulnerabilities of ad-hoc network are due to the challenging issues that also exist in wired networks, such as:

- Passive Eavesdropping
- Man in the Middle Attack
- Intrusion
- Denial of Service

From the problem definition and security threats, it follows that it is needed to secure the communication in this network due to various sensitive applications. The focus of this research is to secure the data communication part of ad-hoc networks.

## 2. Ad-hoc Networks

Ad-hoc networks are becoming popular for their unique characteristics. To achieve the attractive features, ad-hoc network should attain distinguished properties such as peer-to-peer among host, multi-hop routing protocol, and the network is autonomous and auto configured [2].

The typical application of Ad-hoc networks can be described as follows:

- Military Networks
- Emergency Services, as shown in Fig. 2
- Collaborative Networks
- Wireless Sensor Networks
- Personal Area Networks and Bluetooth

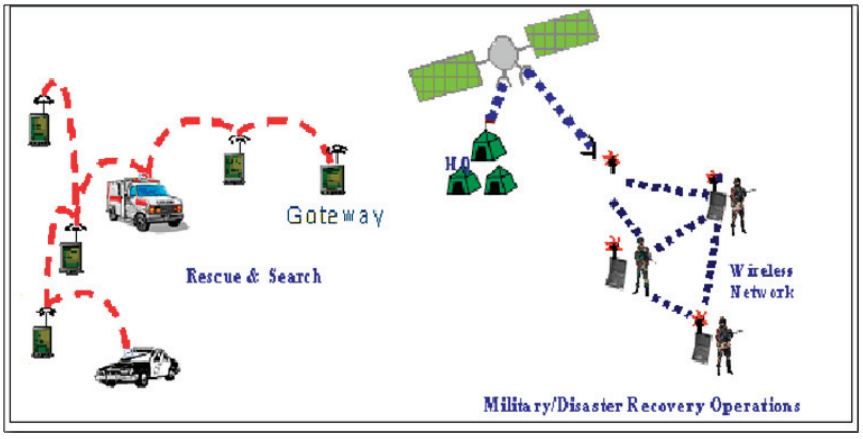


**Fig. 2. Ad-hoc Networks applications.**

When the concept of Ad-hoc network was first established, a set of initial goals was fixed. These goals were scalability, quick convergence, bi-directional communication, loop freedom and unicast. But with the rapid proliferation of ad-hoc networks in different applications, the applications require some other properties such as:

- **Secure routing and data transfer:** Nodes are generally in mobile nature in ad-hoc networks. Currently all routing protocols cope with the dynamic topology without adequate security measure. Therefore, a node may be compromised at any time. As the network serves various sensitive applications, secure routing protocol and secure data transfer mechanism are essential for this network.

- **Quality of service (QoS):** QoS is defined as the ability of a network element such as node to provide some level of assurance for a consistent data delivery. It is a set of service requirements to be met by the network while transporting a packet stream from source to destination. Due to the dynamic nature, limited resource availability and insecure medium, it is needed to maintain QoS for ad-hoc networks.

- **Service discovery:** Nodes may want to get any service from the wireless network on ad-hoc basis in emergency such as in battlefield or rescue operations. Node may search for service after discovery of the route. That is why ad-hoc network need to provide service discovery process for the mobile node in the network [3].

## 3. Routing in Ad-hoc Networks

In ad-hoc networks we have a good number of routing protocols, which are broadly classified into two categories. The first category is Reactive routing or Table Driven, and the second one is Proactive routing or Source Initiated on Demand. In reactive approach, routing information is stored and maintained before the actual transmission begins. From the application perspective, it has the advantage of minimum initial delay as the desired route is already established. Destination-Sequenced Distance-Vector Routing (DSDV) and Wireless Routing Protocol (WRL) are examples of reactive routing [4]. The proactive routing or 'source initiated on-demand' routing protocols create routes only when a source needs to communicate with another node whose path is not known to the source. Ad-hoc On-Demand Distance Vector (AODV) and Dynamic Source

Routing (DSR) are examples of this type of routing. Some routing protocols applied the combination of both reactive and proactive routing. Zone Routing Protocol is such a protocol [5].

Ad-hoc On-Demand Distance-Vector (AODV) routing protocol is specifically designed for mobile ad-hoc wireless network [6]. It provides very quick and efficient route establishment between communicating nodes. In most of the protocols, the overhead is incurred by the fact that each transmitted packet contains the source route to the destination information.

AODV protocol eliminates this problem by maintaining only the next hop information to reach a particular destination. So routing message does not have an increasing size [7]. A monotonically increasing sequence number is used to prevent replay attacks and to ensure loop free routing among the nodes. This scheme of routing is employed in the subsequent simulation model.

## 4. IPSec Architecture

IPSec uses two protocols to provide all its services:

**a. Authentication Header (AH):** This header is added with IP datagram to ensure the integrity and authenticity of the data packet.

**b. Encapsulating Security Payload (ESP):** This header is added to protect the confidentiality, integrity and authenticity of data packet [8].

IPSec uses Security Association (SA) to define a secure link from source to destination. Defined in RFC 2401 a Security Association (SA) is a simple connection that affords security services to its traffic [9].

## 5. Simulation Model

The proposed IPSec implementation is simulated in ad-hoc network environment. The Network Simulator (NS-2) [10] has been chosen for this purpose due to its popularity in the field of wireless networks simulation compared to other simulators [11].

Different parameters have been chosen for creating the simulation environment for our model. Here some static parameters are chosen for set the NS-2 environment and some static data parameters have been chosen for simulating both authentication header and encapsulation

security payload of IPSec [12]. One of the most important parameters is routing protocol, which has a big effect on processing time and delay.

The following static parameters are set for the purpose of simulation.

For the packet sizes, the simulation model assumes the following:

### 1) Packet Size for AH

- Packet Size without AH 1024 bytes.
- Packet Size with AH 1044 bytes (data packet 1024 bytes + SPI 4 bytes + next header 1 byte + payload length 1 byte + reserved 2 bytes + Sequence no. 4 bytes + authentication header 8 bytes).

### 2) Packet Size for ESP

- Packet Size without ESP 5120 bytes.
- Packet Size with ESP 5133 bytes (data packet 5120 bytes + SPI 4 bytes + Padding 1 byte + Authentication 8 bytes) [13].

**Table 1. Static Parameters for NS-2 Simulation.**

| Parameter | Value |
|---|---|
| Size | 600m × 500m |
| Number of nodes | 30 |
| Node placement | Uniform |
| Protocol | 802.11 |
| Antenna type | Omni directional |
| Mobility model | Random waypoint |
| Routing protocol | AODV |
| Packet type | TCP,UDP |

## 6. Results

A snapshot of NS-2 model is shown in Fig. 3. The figure shows 30 mobile nodes which are moving in a random fashion model. Each node has its own direction in the two dimensions topology. For example, node number (0) moves from its initial location which is x-axis = 0 and y-axis = 0 to the location x-axis = 50 and y-axis = 350 after 10 seconds with high velocity.

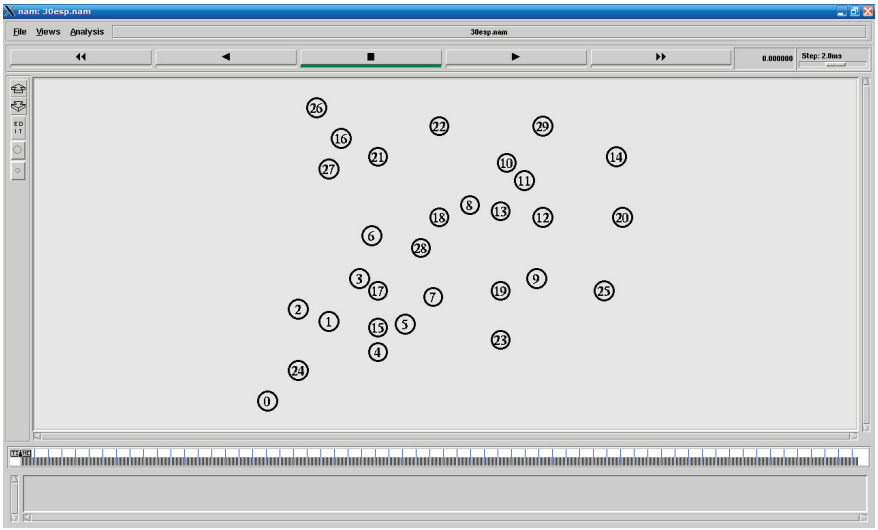


**Fig. 3. Snapshot for the simulated environment by NS-2.**

Data has been collected from fixed number of nodes within the assumed 30 nodes ad-hoc network environment. Figures 4-7 show that the simulated ad-hoc network with ESP has more throughput, processing time, delay and jitter than the same network with AH protocol [14].

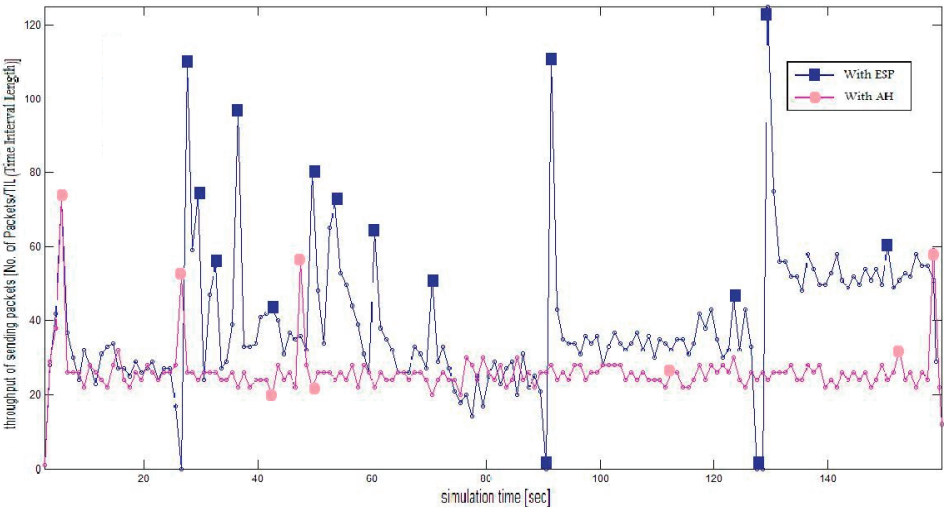


**Fig. 4. Throughput of sending packets with AH and with ESP.**

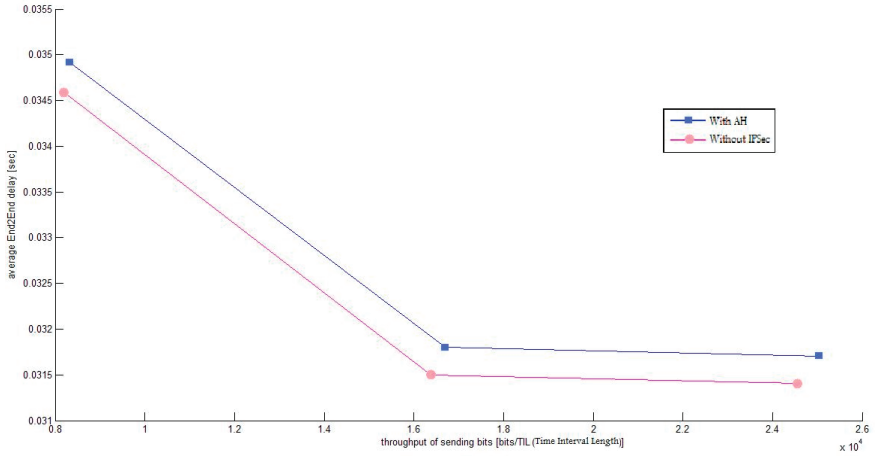


**Fig. 5. Throughput of sending bits vs. average end to end delay with AH and without using IPSec.**

Comparing ESP with AH, ESP provides more services compared to AH such as confidentiality of data packet by encryption. Therefore, it depends upon the user to choose the level of security that he needs for transmitting data packet among nodes in ad-hoc networks. If highest security is required for any data packet then the choice should be ESP and if authenticity is required rather than confidentiality then this can be achieved by using AH.

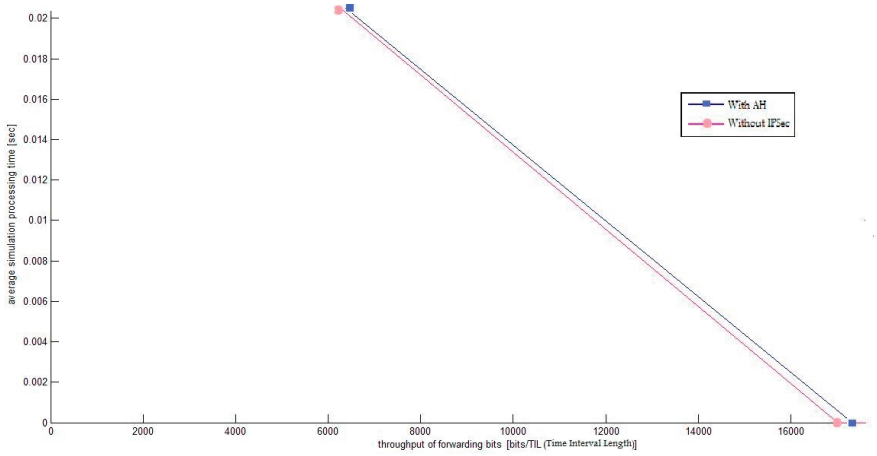


**Fig. 6. Throughput of forwarding bits vs. average processing time with AH and without using IPSec.**

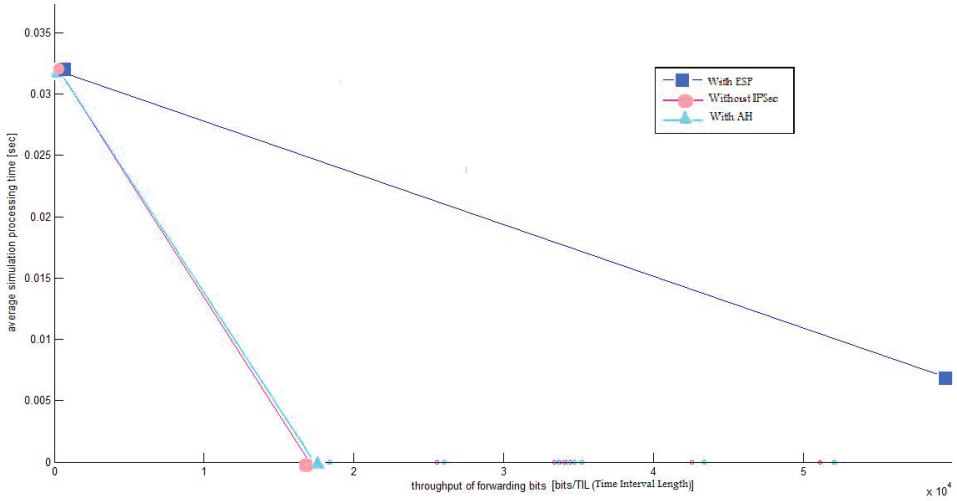


**Fig. 7. Throughput of forwarding bits vs. average processing time with ESP, AH and without using IPSec.**

## 7. Conclusion

Due to various emergency and sensitive applications, data packet security needs to be achieved in ad-hoc networks, but guaranteeing complete security in such a network may be impossible if the nodes are too mobile and suddenly compromised. The proposed IPSec implementation attempts to ensure data communication security.

Sending and receiving data packets with IPSec needs more time as compared to sending data packets without IPSec. Between AH and ESP implemented data packets, ESP implemented data packets consume more time due to handling encryption.

If an application needs only authentication, simulation shows that AH-implemented data packets have minimum time overhead. Results also encourage implementing IPSec with ESP for all security services with moderate time overhead.

There are ongoing modifications of Ad-hoc On-Demand Distance-Vector routing protocol (AODV) to fulfill the security requirements. The security proposal of this research is just the beginning of work in the area of data communication security in ad-hoc networks. Implementation of Encapsulating Security Payload (ESP) and Authentication Header (AH)

of IPSec ensure confidentiality, authenticity of data and as a result, security will be further improved.

**References**

[1] **Ilyas, M.,** "*The Handbook of Ad-Hoc Wireless Networks*", CRC Press (2003).

[2] **Basagni, S., Conti, M., Giordano, S.** and **Stojmenovic, I.,** "*Mobile Ad hoc Networking*", John Wiley & Sons, Inc. (2004).

[3] **Bayya, A. K., Gupta, S., Shukla, Y. K.** and **Garikapati, A.,** "*Security in Ad-Hoc Networks*" (2003).

[4] **Royer, E. M.** and **Toh, C.K.,** "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", *IEEE Personal Communication* (1999).

[5] **Anjum, F.** and **Mouchtaris, P.,** "*Security for Wireless Ad Hoc Networks*", John Wiley & Sons, Inc., ISBN 978-0-471-75688-0, (2007).

[6] **Zapata, M. G.** and **Asokan, N.,** "Securing Ad Hoc Routing Protocols", *Proc. ACM Workshop on Wireless Security (WiSe*), ACM Press (2002).

[7] **Zhou, L.** and **Haas, Z.J.,** "Securing Ad Hoc Networks", *IEEE Network Magazine* (1999).

[8] **Doraswamy, N.** and **Dan Harkins,** " *The New Security Standard for the Internet, Interanets, and Virtual Private Networks"*, Second Edition, IPSec (2003).

[9] **Ghosh, A., Talpade, R., Elaoud, M.** and **Bereschinsky, M.,** "Securing Ad-hoc Networks Using IPSec", IEEE *Military Communications Conference,* MILCOM (2005).

[10] **The Network Simulator NS-2,** http://www.isi.nsnam.com/ns/

[11] **Cavin, D., Sasson Y.** and **Schiper, A.,** "*On the Accuracy of MANET Simulators*", Distributed Systems laboratory (2004).

[12] **Ros, F. J.** and **Ruiz, M.P.,** "*Implementing a New MANET Unicast Routing Protocol in NS2*", Sun Microsystems Inc., (2004).

[13] **Islam, S.,** "*Implementation & Comparison of IPSec Protocols for Secure Data Communication in Ad-Hoc Networks*", Royal Institute of Technology, (2006).

[14] **NS-2 Analyzer and Trace Graph,** http://www.tracegraph.com/

# محاكاة بروتوكول الأمان IPSec على الشبكات اللاسلكية Ad-hoc

**أحمد عدس، و توفيق شاولي**

*قسم الهندسة الكهربائية وهندسة الحاسبات، كلية الهندسة، جامعة الملك عبدالعزيز، ص.ب. ٨٠٢٠٤، جدة ٢١٥٨٩، المملكة العربية السعودية*

*المستخلص.* يعد تكاثر أجهزة الحاسب المتنقل وأجهزة الاتصالات بهذه السرعة تغييرًا جذريًا في مجتمعنا التقني، فنحن الآن ننتقل من عصر الحواسب الشخصية إلى عصر الحواسب المستخدمة في أي مكان والوصول إلى المعلومة المطلوبة في أي وقت وبسرعة هائلة. تمثل الشبكات اللاسلكية المتنقلة من النوع Ad-hoc أنظمة توسعية معقدة تشتمل على أطراف لاسلكية متنقلة تنشأ ذاتيًا بصورة ديناميكية وبشكل مؤقت. طبوغرافيات الشبكة Ad-hoc تمكن الأشخاص والأجهزة من الاتصال ببعضهم البعض بدون وجود بنية تحتية معدة مسبقا للاتصال وبدون مركزية.

في بيئة الشبكات اللاسلكية من النوع Ad-hoc نحتاج إلى المزيد من الجهد لزيادة الأمان في الشبكة، ففي الوقت الحالي يوجد لدينا العديد من بروتوكولات التوجيه المقترحة والمطبقة أيضًا ولكن بدون ضمان آلية أمان حقيقية. على سبيل المثال البروتوكول AODV يكاد يكون هو البروتوكول القياسي في التوجيه ورغم ذلك فالباحثون يفكرون الآن جديًا في أمان هذا البروتوكول، فنقص الدعم فيما يتعلق بالبنية التحتية وحساسية الاتصالات اللاسلكية يسببان قلقًا وخوفًا شديدين من أمان هذا النوع من الشبكات.

أيضا هناك الكثير من التحديات التي تواجه الباحثين مع الشبكات اللاسلكية من النوع Ad-hoc بالإضافة إلى ضمان أمن الشبكة وهي كالتالي:

- الطبوغرافيات الديناميكية بدون سلطة مركزية.
- الموجة المعاقة.
- المصادر المحدودة.
- اتصال البيانات الآمن.

تم في هذا البحث تنفيذ بروتوكولات نظام الأمن IPSec على الشبكات اللاسلكية من النوع Ad-hoc، كما تم محاكاة واختبار النظام على برنامج المحاكاة NS-2 لضمان أفضل نظام أمان لهذا النوع من الشبكات.