

## Simulation of Cryptographic Algorithms in IPSec on Ad-Hoc Networks

A.A. Adas and A. A. Alsharif

*Department of Electrical and Computer Engineering, Faculty of Engineering, KAU, P.O.Box 80204, Jeddah 21589, Saudi Arabia*

*aadas@kau.edu.sa*

**Abstract.** This paper focuses on secure data communication between nodes in Ad-Hoc networks by employing IPSec (Internet Protocol Security). In wireless communication, Ad-Hoc network is a new paradigm since, which is used for highly sensitive and emergency operations. Ad-Hoc network is considered a number of mobile nodes that are connected through wireless interfaces and moves arbitrarily. Ensuring security is one of the main issues due to its infrastructure less solutions. This research aims for IPSec protocol that provides security for an Ad-Hoc networking in a various applications. IPSec incorporates security model, *i.e.* AES (Advanced Encryption Standard) into its framework. In this work, we consider the problem of incorporating security mechanisms to securing data communication for Ad-Hoc networks. We look at AODV routing protocol (Ad-Hoc On-Demand Distance Vector) in detail and it is used for secure routing. Simulation of IPSec protocol is simulated using NS-3 simulator. Results from NS-3 simulator is compared with AH, ESP, and AES in terms of Quality of Service parameters throughput, average processing time and average end-to-end delay.

**Keywords:** IPSec, AH, ESP, AES, Ad-Hoc networks.

### 1. Introduction

Nowadays, the information technology and information technology based industries used wireless networks since wireless networks have been well widely deployed and it provide high-speed Internet access to mobile users. Most of the wireless network uses access points to access the Internet. In a real time network scenarios, where mobile users can access the network through both systems, *i.e.* public mode systems and IP based wireless systems. Currently there are two types of mobile wireless networks are used that are Infrastructure networks and Ad-Hoc networks<sup>[1]</sup>. Infrastructure networks have fixed infrastructure and fixed gateways. These networks bridges are known as Base stations. A mobile unit /device is communicated with the nearest access point (within the coverage area). Access points allow sharing the Internet connection to other

mobile users. Ad-Hoc networks are infrastructure less networks which don't have any fixed routers, access points and base stations. All nodes in this network can be moved with dynamic and arbitrary manner. The typical structure of infrastructure and Ad-Hoc networks are illustrated in Fig.1. The possibility for wireless access is a very important aspect of "Ad-Hocness". Wireless Ad-Hoc use of the communication infrastructure imposes many newly available requirements on both mobility management and security of the wireless system. This is especially done in Ad-Hoc network type of operations since it allows users to operate public network operators to paying subscribers. Generally, wireless access to the network cannot be restricted physically and cryptography methods are used to protect the transmitted data and network elements. In addition, the used of IP-based infrastructure is

used to similar to about and the following aspects are considered in IP-based infrastructure: Data confidentiality, data authenticity and data integrity and service availability. Currently the available standards offers some complementary mechanisms for creating secure data communication with optional data encryption and packet authentication over the wireless links that are IEEE 802.11 wired equivalent privacy (WEP) and IPSec. A wireless Ad-Hoc network is computer network in which the communication links are wireless. Ad-Hoc networks are communicating between the nodes by wireless links, which do not necessarily rely on any fixed infrastructure. Nowadays Ad-Hoc networks are widely used in mobile applications with relatively low cost and attain high performance. Wireless link is susceptible to attacks, a security becomes very important task in Ad-Hoc networks.

One of the common issues in *Ad-Hoc* network is security. There is a number routing protocols have been proposed to improve the security of network [2]. But the all the routing protocol does not ensuring proper security mechanism. AODV is one of the routing protocols which highly concentrate by researches to use for security in *Ad-Hoc* network. Moreover, for ensuring security of an infrastructure less *Ad-Hoc* network, the following sets of issues are facing the researchers [3]:

- No fixed access points
- Dynamic network topology
- Limited bandwidth
- Contrary environment
- Irregular connectivity of nodes
- Secure data communication
- Limited resources

- Peer-to-peer architecture with multi-hop routing

Due to the following reasons, an *Ad-Hoc* network may affects the security threats or attacks:

- Intrusion
- Denial of service
- Eaves dropping (passive attacks)
- Data corruption, worms and viruses
- Active inference
- Man in the middle attack
- Hello flood and black hole

In order to implement a secure *Ad-Hoc* network, the following functionalities should concern:

i) Data confidentiality: When mobile users connect with wireless interfaces, information between users required to keep as a private. Since unauthorized or third party persons can access the information. This is needed to be accomplished through encryption by both public as well as private.

ii) Data integrity: In a given coverage area, transmitted data cannot be modified in transit due to any error or third party access. This characteristic accomplished by HFs (Hash Functions) and MACs (Message Authentication Codes)

iii) User authentication: Users within a coverage area must provide any certificate proof of their identity. Since it may useful for identifying the users either authorized user or unauthorized user. However, unauthorized user may access the information. This will accomplished by digital signatures [3].

From the above mentioned problem, challenges, issues and security characteristics, *Ad-Hoc* network must be requires for secure model to secure the data communication. The

major contributions of our work are as follows:

- The proposed work focuses on secure data communication in *Ad-Hoc* networks.
- Design cryptographic algorithm to enhance the performance of security mechanism

- Protecting routing information through effective routing

The paper is organized in such a way that Section 2 discusses about the related work. Section 3 discusses the *Ad-Hoc* networks, Section 4 describes routing in *Ad-Hoc* networks, Section 5 discusses IPSec framework, Section 6 illustrates simulation model, and finally Section 7 gives the conclusion.

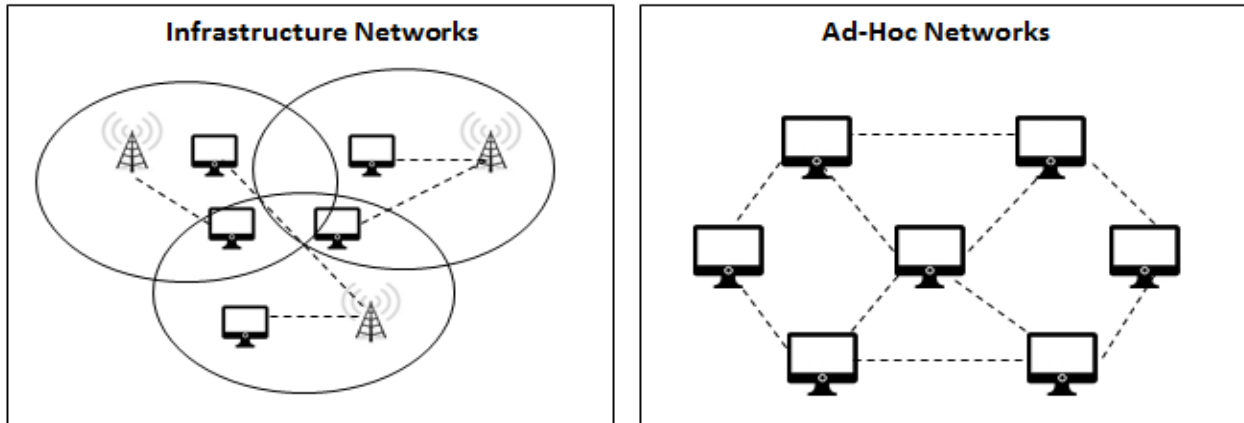


Fig. 1. Infrastructure networks and Ad-Hoc networks.

## 2. Related Work

This section explains some existing works in the literature revised by various country researchers including various protocols, techniques and methods works under security in Ad-Hoc network.

Kandhil and Kumar <sup>[4]</sup> proposed IPSec protocol for secure data communication after route establishment in Ad-Hoc network. IPSec works on network layer of the OSI and the TCP/IP. When running IPSec on layer 3, it is able to function transparently for applications running on application layer. In this work, IPSec protocol provides end user traffic with ensuring authentication and data confidentiality of data packets. It also includes protocols for establishing mutual authentication between agents.

Vesa Karpijoki <sup>[5]</sup> discussed security in Ad-Hoc networks, in which many of the new generation and currently available security mechanisms are discussed. Generally, an Ad-Hoc network sets new challenges for the necessary security architecture. The brief studies of this research are listed as follows: Network infrastructure, networking operations, physical security, data availability, data access control, criteria's for protecting Ad-Hoc networks, and security threats in Ad-Hoc networks.

Rahman <sup>[6]</sup> investigated the performance of mobile Ad-Hoc networks by applying IPSec protocol. In this work, Riverbed Modeler Academic Edition Simulator is used for investigating network performance. The comparison is done by with IPSec protocol and without IPSec protocol, in which Network with IPSec attains high performance when

compared with network without IPSec protocol. In addition, a MANET with attack is overcome by AODV routing protocol.

Panaousis *et al.* [7] proposed adaptive and secure routing protocol for emergency mobile Ad-Hoc networks. This protocol is used for various emergency situations like forest fires, terrorist attacks and earthquakes. These networks perform well in such situations and the performance is analyzed in terms of node mobility levels, node transmission radius, battery level of nodes data load, traffic requirements, wireless link quality, and network size.

### 3. Ad-Hoc Networks

*Ad-Hoc* networks are very popular network, which have unique characteristics to work in environment. To achieve the attractive unique features, *Ad-Hoc* network should attain the distinguished properties, such as multi-hop routing, self-creation, self-organization and self-administration, physical security, network scalability, autonomous and infrastructure less, device heterogeneity, energy constrained operation, bandwidth constrained variable capacity links, and dynamic network topology [8].

The application of *Ad-Hoc* networks are as follows (Fig. 2):

- Tactical networks- Military communication and operations and automated battle fields.
- Emergency services – Disaster recovery and search and rescue operations.
- Commercial and civilian environments: E-commerce, business, sports and vehicular services.
- Home and enterprise networking- Home, and office wireless networking.

- Education- Universities and campus settings.

- Entertainment- Multi-user games and outdoor Internet access.

- Sensor networks – Home applications.

Once the *Ad-Hoc* network is deployed the set of goals of network is required to fix such as network scalability, bi-directional communication, quick convergence, unicast, and loop freedom. An *Ad-Hoc* network defines some qualitative properties for assessing performance or suitability of a routing protocol. Some of the properties of Ad-Hoc Networks are [8]:

*Secure routing and Data Transmission:* *Ad-Hoc* routing protocols are exposed to many kinds of security attacks. The possibility of eavesdropping, DoS and spoofing attacks is higher in *Ad-Hoc* network. Mobile users can move arbitrarily with respect to other nodes in the network. Since dynamic topology can affect the security measure. Therefore, secure routing protocol and data transmission mechanism are necessary for this *Ad-Hoc* network [9].

*Key Management Service:* Key management service is always required for *Ad-Hoc* networks. Cryptographic schemes such as digital signatures to protect both routing information and data traffic information. But the single certificate authority and trusted authority is not sufficient for entire secure operation. Therefore, a standard approach is required to improve the performance of network availability.

*Quality of Service (QoS):* QoS is defined as the performance level of a service that offered by the network to the mobile user. QoS consists of set of requirements that are met by the network and the requirements characterized to bandwidth, jitter, delay, packet delivery

ratio, and communication overhead. For QoS provisioning, resource limitations has occurred

#### 4. Routing Protocols in Ad-Hoc Networks

The fundamental idea of a routing protocol in *Ad-Hoc* network is to deliver the messages from source node to destination node with enhanced the network performance in terms of security and delay. The major goals of routing protocols are minimal control overhead, minimal processing overhead, multi-hop routing capability, dynamic topology maintenance, and loop prevention. Many routing protocols have been developed for *Ad-Hoc* networks. *Ad-Hoc* routing protocols have been classified in to two types<sup>[10]</sup>:

- Table Driven Routing Protocols or Pro-active Routing Protocols.

- Source Initiated Demand Driven or Reactive Routing Protocols.

##### (i) *Table Driven Routing Protocols or Pro-active Routing Protocols*

These types of protocols used pro-active approach for perform routing in *Ad-Hoc* networks. They attempt to maintain consistent, up-to-data routing information from each and every node in the *Ad-Hoc* network. Table driven protocols require each and every node to maintain one or more routing tables to store the information of routing, also the changes should be reflected on routing table and changes in the network topology or movements in source node.

##### (ii) *Source Initiated Demand Driven or Reactive Routing Protocols*

These routing protocols eliminate the conventional routing tables and consequently reduce the need for updating these tables to track changes in the network topology. When a node requires a route to a destination, it first initiated a route discovery process within the network. This process is stopped once a route

is found. Some of the reactive routing protocols are as follows: DSR, ABR, PAR, SSR, LAR, CBR, TORA, and AODV. Reactive protocols are more efficient at signaling and power consumption. The classification of protocols are shown in Fig. 3.

AODV is a reactive unicast routing protocol for *Ad-Hoc* networks. Among the reactive routing protocol, AODV only needs to maintain the routing information (routing table) about the active routing paths. The major functionalities of AODV are dynamic, self-starting, multi-hop routing between participating nodes interesting to establish and maintain an *Ad-Hoc* network. This routing protocol allows nodes in network to obtain paths quickly to reach the new destinations. It does not require mobile nodes to maintain and manage routing paths to destinations. In a timely manner, AODV protocol allows mobile nodes to respond to link breakages and modify the network topology<sup>[11]</sup>.

Our main aim is to find a secure routing protocol that can be implemented on AODV without degrading the performance of quality of service of *Ad-Hoc* networks. When a source code requires to sending message to destination node, the route is discovered. So it first initiates the process of route discovery. In this step, source node broadcasts a route request message (RREQ) to its neighbor's node, until the desired route is find for destination. AODV routing protocol utilizes the destination sequence numbers to ensure all routes are loop free and contain the most recent route information. Each node maintains its own sequence number and the broadcast ID in routing table. During the process of forwarding RREQ from source to neighbor's node, intermediate nodes record in their route tables the address of the neighbor from, which neighbor nodes is received the first copy of the broadcast packet, thereby establishing the reverse path. Later copies of the RREQ

received nodes are discarded once the first copy of the node identified. Once the RREQ received to the destination node or any intermediate node, immediately responds the destination or intermediate node by unicasting a RREP packet to the neighbor node [First

received RREQ node]. If a source node moves, it is able to reinitiates the process of route discovery. Based on this, routing is performed. Figures 4 and 5 describe about RREQ route propagation and RREP route path of AODV routing.



Fig. 2. Typical applications of Ad-Hoc networks.

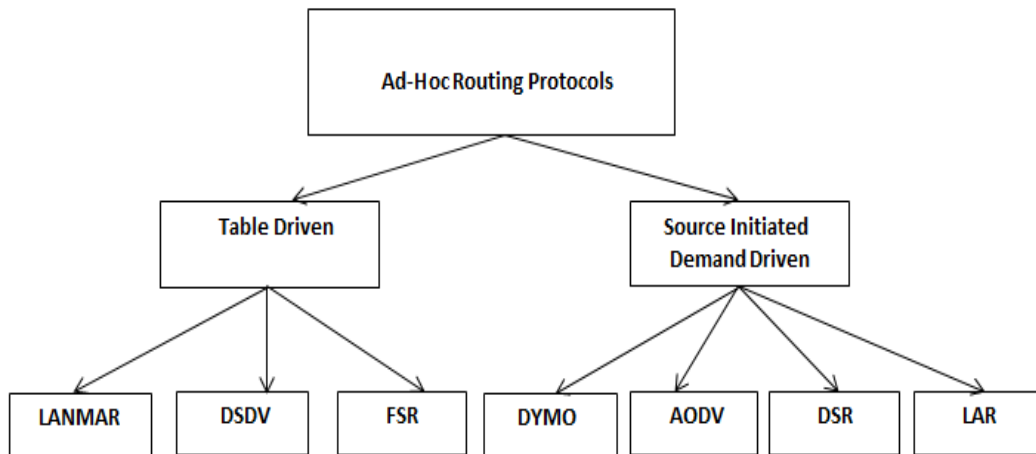


Fig. 3. Routing protocols in Ad-Hoc Networks.

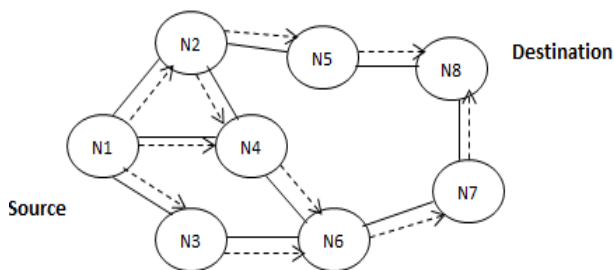


Fig.4. Propagation of RREQ.

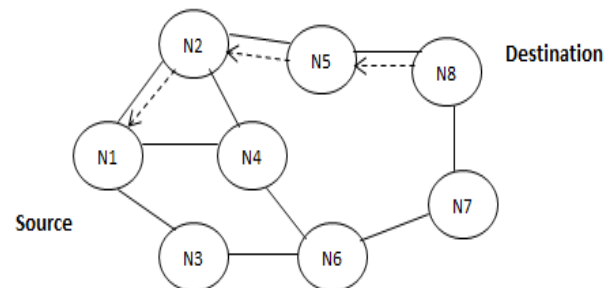


Fig. 5. Route path [reply from destination].

## 5. IPSec Framework

IPSec is a standard for providing security at the *Ad-Hoc* networks. It facilitates the authentication of the communicating entities allows them to setup secure IP channels for data exchange and provides a secure framework for the employment of different cryptographic algorithms depending on the level of security required by the users and their applications.

IPSec protocol provides two security protocols for protecting the data more secure:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Authentication header protects data with an authentication algorithm and ESP protects data with an encryption algorithm. ESP can be used with an authentication mechanism. Otherwise we can use ESP for both authentication and an encryption algorithm. But in our work, we proposed AES which provides encryption and authentication within a single algorithm.

IPSec provides an open framework for incorporating a wide range of different cryptographic algorithms for the actual cryptographic task of transforming the original plain text messages into the transmitted cipher text. Most encrypting algorithms are used in IPSec. They break the user's original data packets into basic blocks of constant size. Then the blocks encrypted independently through a number of encryption cycles. Ciphers depend upon the choice of block size key size and the number of cycles. When the "block size" is getting larger that means it will produce greater security but the speed of the encryption and decryption process will be reduced. Similarly, larger "key size" may lead to greater security but also reduce the speed of encryption and decryption. A "number of cycles" metric is usually used for specifying

the number of repetitions of the common encryption process on each block data <sup>[12]</sup>.

To overcome the aforementioned issues, we proposed AES cryptographic algorithm for encryption and authentication. Figure 7 shows the flow of AES encryption algorithm. AES refers to advanced encryption standard. The key size used for an AES cipher specifies the number of repetitions of transformation rounds, that convert the input, *i.e.* plain text in to the output called cipher text. AES encrypts block size of 128-bit. AES comprised of four transformations, such as addroundkey transformation, subbytes transformation, shiftrows transformation, and mixcolumns transformation. These four transformations are a unit of AES algorithm called "Round". Round repeats basically and the number of repeat *Nr* depends upon the key size. Key size is extended depending on the number of *Nr*. The numbers of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

The main advantages of AES mentioned in below:

1. Simplicity of design: The cipher text does not base of security and also not well understood interactions between arithmetic operations.
2. Block length variations: The variable block size allows the construction of a collision-resistant iterated hash function.
3. Extensions possibility: The number of rounds or cycles is fixed in the specifications and it increased in case of security problems.
4. More secure encryption/decryption system: The expanded key is always derived from cipher key.

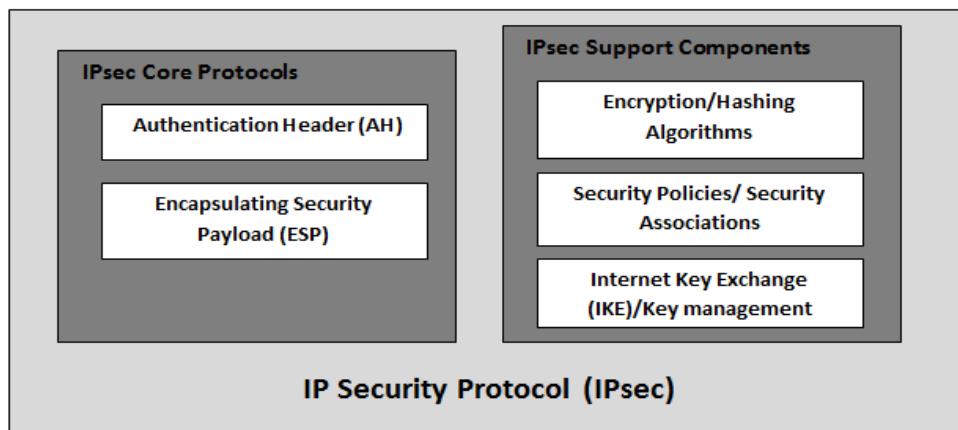


Fig. 6. IPsec Protocol Architecture [12].

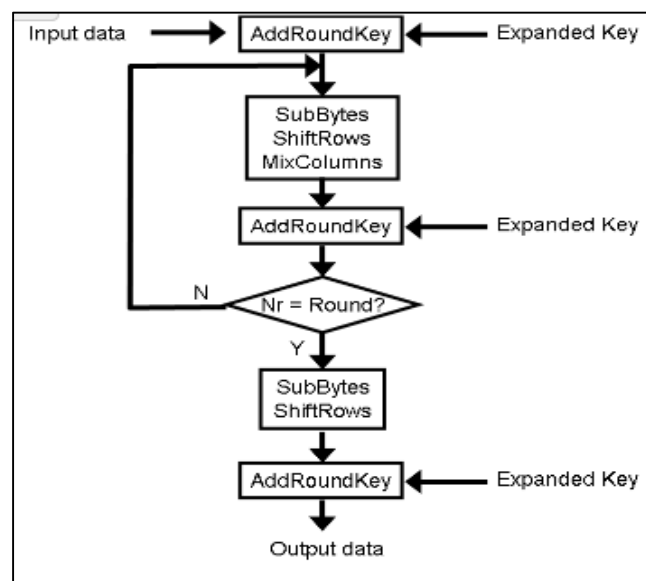


Fig. 7. Flowchart for AES.

By using AES encryption algorithm in IPsec protocol, it provides four basic aspects of information security:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

## 6. Simulation Environment

The simulations have been performed using NS-3 simulator that provides scalable simulation of wireless networks. NS-3 is a

discrete event simulator mostly used for research in networking. NS3 used for both wire and wireless network protocol and also with their function. NS-3 provides substantial support for simulation of TCP, routing and multicast protocols in wired and wireless (local and satellite). NS-3 is written in two languages: C++ and python. It is the open source software, which deals with the performance of various network protocols and evaluates new protocols before use.



As mentioned in Table 1. Our consideration in network with the size of 50 nodes and each node randomly moves with in a simulation area of 600\*500 M. Our network always uses omni directional antenna as antenna type and use Mac layer as IEEE 802.11 Mac layer. The nodes are moved in random way point direction, since we applied random waypoint model. Here each node starts from a random location to a random speed with uniformly distributed between 0 and a maximum speed of 300 Mbps.

**Table 1. Simulation parameters and values.**

Simulation Parameters	Value /Range
Network size	600m × 500 m
Number of nodes	50
Node placement	Uniform
Protocol	802.11
Antenna Type	Omni Directional
Mobility Model	Random Waypoint model
Routing Protocol	AODV
Packet type	TCP, UDP

## 6.1 Performance Analysis

In this subsection, network performance was analyzed. We use the following three simulation parameters to analyze the performance of our proposed work with the existing ones:

(i) *Throughput*: It is the total number of packets delivered over the total simulation time. It measures how well the network can constantly provide data / packet to the destination. Throughput is defined by Mbps and for achieving better performance is should be in high.

$$\text{Throughput (\%)} = \frac{\text{Number of sent packets}}{\text{Time taken}} * 100 \quad (1)$$

(ii) *Average Processing Time*: Average processing time is defined as the total simulation time for processing the data packets from source to the destination.

$$\text{Average processing time} = \frac{\text{Sum of time}}{\text{Received packets}} \quad (2)$$

(iii) *End-to-end delay*: The average end-to-end delay of a data packet is the total amount of transmission delay of packets. It consists of propagation delays, queuing delay, retransmission delays.

$$\text{Average end to end delay} = \frac{\text{Delay Sum}}{\text{Received Packets}} \quad (3)$$

The parameters that are mentioned above are very important determinants and quality of service parameters of network performance. We have done this paper to imply that our proposed IPSec protocol with AES enhances the security of AODV routing protocol without degrading the performance of the network.

## 6.2 Simulation Results

In this section, a snapshot of NS-3 model is shown and this model constructed with 50 nodes, which are moving in a random fashion model. Figures 8-13 show the NS-3 simulation snapshots of *Ad-Hoc* network for IPSec with AES. The proposed model is constructed with 50 nodes, and the creation of nodes and simulation environment is shown in Fig. 8 and 9 respectively. After deploying, AES is processed in which key size (length) is chosen for simulation. In our proposed work, we have considered key size is 128. Finally, IPSec simulation is started.

Data has been collected from fixed number of nodes within the assumed 50 nodes *Ad-Hoc* network environment. Figures 14-16 show the snapshots of the *Ad-Hoc* network simulation results for IPSec with AES in terms of throughput, processing time, and end-to-end delay. The performance of the AH, ESP and AES were differs based on the size of the data. AH uses (24 Byte header) whereas ESP uses (8 Byte header, 16 Byte trailer and 16 byte IV). AES uses 128 bits for data communication. The system will achieve

better performance in terms of throughput, processing time, and end-to-end delay. However the processing time is essential and it should minimum for better network performance. When encrypting packets, these two, *i.e.* AH and ESP, takes high time. The comparative simulation results for AH, ESP, and AES varying for network sizes. The simulation results can be discussed and explained in below.

### 6.2.1 Throughput

This performance metric is significant to be considered while designing different algorithms in the network. Throughput is improved if the routing protocol performs perfectly with respect to its design.

Figure 14 shows that our proposed is better than the previously used techniques. Since we have designed a novel routing protocol, which selects shortest path for data transmission and also a major reason for using this routing protocol is which improves the throughput of the network. Due to this reason, there is a high throughput even when the number of nodes increases. Due to the better performance of AH and ESP, throughput is similar to our proposed IPsec AES algorithm.

### 6.2.2 Average End-to-End delay

Delay is a performance metric, which should be measured for showing better performance in our work. Delay in data transmission is caused due to the poor design of routing protocol.

Figure 15 implies the comparative result of delay, in which our proposed protocol has greatly reduced delay, (*i.e.* Mobility (Bytes per Unit Time), whereas in previous work the delay increases when the number of nodes keeps on increasing. On decreasing delay in our AODV protocol adds up a positive constraint to attract more users to use this protocol. Our proposed protocol reduces delay,

due to the perfect selection of route. Routing in AODV is identifying a route for data transmission. Other routing protocols were not able to tolerate in case of unauthorized user access.

### 6.2.3 Average Processing Time

Figure 16 shows that our proposed is better than AH and ESP. AES algorithm reduces the processing time of data packets. The processing time is varied for various key sizes, such as 128, 192 and 256. Comparing ESP, AH with AES, AES provides more services [confidentiality of data packets] when compared to ESP and AH. In addition, AES achieved higher security, confidentiality and authenticity for any data packet rather the ESP and AH. AES algorithm gives better performance for encryption and message authentication. AH and ESP has three functionalities confidentiality, data integrity and authenticity. But AES provides confidentiality and authentication together efficiently. In our simulation for varying number of nodes so the number of rounds of simulation is also gets varied. As we can see in Fig. 16, at round 4000 the average packet processing time for AES is 0.0015 seconds.

## 7. Conclusion

Due to the rapid developments in the field of *Ad-Hoc* networking, the nodes needs to form a self-creating, self-organizing and self-administering wireless network. But the network, must guaranteeing the set of QoS requirements. This paper presents the design, implementation and comparison of the secure data communication IPsec protocol in the network simulator NS3, and analyzes the performance of network in terms of throughput, average processing time and average end-to-end delay. The proposed IPsec with AES implementation attempts to ensure data communication security. When we increase the length of key size, AES gives

strong resistance against the security threats and attacks, and it has an acceptable speed of data encryption and decryption. When we combine IPSec with AES, the *Ad-Hoc* network is more secured. In order to route data packets AODV is proposed. The presented simulation

results quantify the differences in throughput, delay and processing time of the AH and ESP of IPSec. In future, we planned to investigate the QoS by applying various parameters, such as jitter, packet delivery ratio, and packet loss rate.

```

projects@master: ~/ns-allinone-3.24.1/ns-3.24.1
projects@master:~$ cd ns-allinone-3.24.1/ns-3.24.1/
projects@master:~/ns-allinone-3.24.1/ns-3.24.1$ sudo ./waf --run IPSecPro --vis
[sudo] password for projects:
waf: Entering directory '/home/projects/ns-allinone-3.24.1/ns-3.24.1/build'
[ 67/2008] Compiling install-ns3-header: ns3/backoff.h
[ 195/2008] Compiling install-ns3-header: ns3/backoff.h
[ 524/2008] Compiling install-ns3-header: ns3/gplot.h
[ 897/2008] Compiling install-ns3-header: ns3/gplot.h
[1859/2008] Compiling scratch/IPSecPro.cc
[1989/2008] Linking build/scratch/IPSecPro
waf: Leaving directory '/home/projects/ns-allinone-3.24.1/ns-3.24.1/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (15.136s)
Packet Size without AH1024bytes,Packet Size with AH 1044 bytes and Packet Size without ESP 5120 bytes Packet Size with ESP 5133 bytes
Could not load icon applets-screenshooter due to missing gnomedesktop Python module
scanning topology: 50 nodes...
scanning topology: calling graphviz layout
scanning topology: all done.

```

Fig. 8. Snapshot of creation of 50-nodes in NS3.

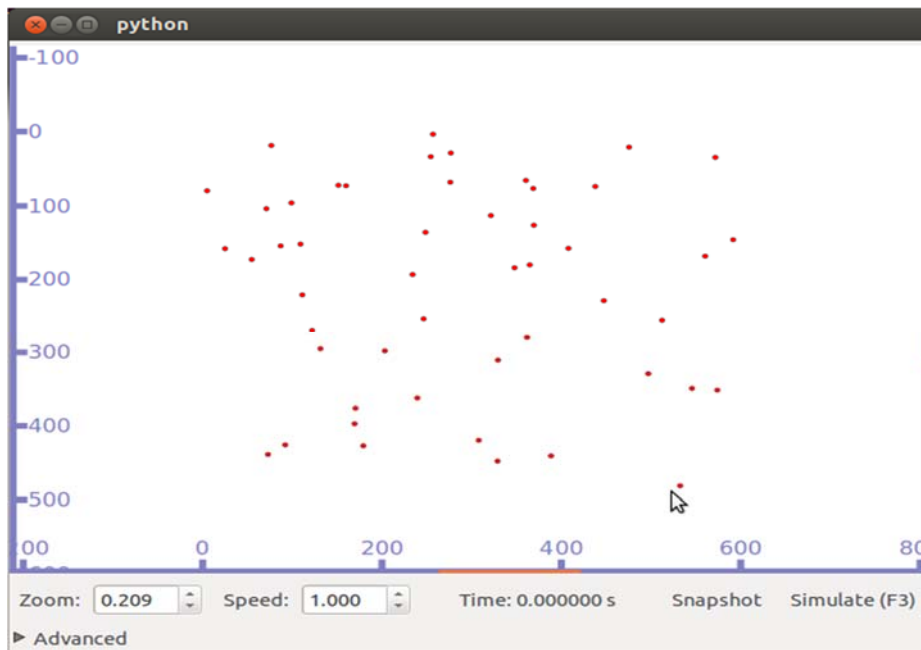


Fig. 9. Snapshot for the simulated environment by NS-3.

```

projects@master: ~/ns-allinone-3.24.1/ns-3.24.1
projects@master:~/ns-allinone-3.24.1/ns-3.24.1$ cd ns-allinone-3.24.1/ns-3.24.1/
projects@master:~/ns-allinone-3.24.1/ns-3.24.1$ sudo ./waf --run IPSecPro --vis
[sudo] password for projects:
Waf: Entering directory `/home/projects/ns-allinone-3.24.1/ns-3.24.1/build'
[ 67/2008] Compiling install-ns3-header: ns3/backoff.h
[ 195/2008] Compiling install-ns3-header: ns3/backoff.h
[ 524/2008] Compiling install-ns3-header: ns3/gplot.h
[ 897/2008] Compiling install-ns3-header: ns3/gplot.h
[1859/2008] Compiling scratch/IPSecPro.cc
[1989/2008] Linking build/scratch/IPSecPro
Waf: Leaving directory `/home/projects/ns-allinone-3.24.1/ns-3.24.1/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (15.136s)
Packet Size without AH1024bytes,Packet Size with AH 1044 bytes and Packet Size w
ithout ESP 5120 bytes Packet Size with ESP 5133 bytes
Could not load icon applets-screenshooter due to missing gnomedesktop Python mod
ule
scanning topology: 50 nodes...
scanning topology: calling graphviz layout
scanning topology: all done.
Enter the length of AES Key(128, 192 or 256 only): █

```

Fig. 10. Snapshot of choosing key size of AES.

```

projects@master: ~/ns-allinone-3.24.1/ns-3.24.1
projects@master:~/ns-allinone-3.24.1/ns-3.24.1$ cd ns-allinone-3.24.1/ns-3.24.1/
projects@master:~/ns-allinone-3.24.1/ns-3.24.1$ sudo ./waf --run IPSecPro --vis
[sudo] password for projects:
Waf: Entering directory `/home/projects/ns-allinone-3.24.1/ns-3.24.1/build'
[ 67/2008] Compiling install-ns3-header: ns3/backoff.h
[ 195/2008] Compiling install-ns3-header: ns3/backoff.h
[ 524/2008] Compiling install-ns3-header: ns3/gplot.h
[ 897/2008] Compiling install-ns3-header: ns3/gplot.h
[1859/2008] Compiling scratch/IPSecPro.cc
[1989/2008] Linking build/scratch/IPSecPro
Waf: Leaving directory `/home/projects/ns-allinone-3.24.1/ns-3.24.1/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (15.136s)
Packet Size without AH1024bytes,Packet Size with AH 1044 bytes and Packet Size w
ithout ESP 5120 bytes Packet Size with ESP 5133 bytes
Could not load icon applets-screenshooter due to missing gnomedesktop Python mod
ule
scanning topology: 50 nodes...
scanning topology: calling graphviz layout
scanning topology: all done.
Enter the length of AES Key(128, 192 or 256 only): 128█

```

Fig. 11. Snapshot of AES for 128 key size.

```

projects@master: ~/ns-allinone-3.24.1/ns-3.24.1
projects@master:~/ns-allinone-3.24.1/ns-3.24.1$ cd ns-allinone-3.24.1/ns-3.24.1/
projects@master:~/ns-allinone-3.24.1/ns-3.24.1$ sudo ./waf --run IPSecPro --vis
[sudo] password for projects:
Waf: Entering directory `/home/projects/ns-allinone-3.24.1/ns-3.24.1/build'
[ 67/2008] Compiling install-ns3-header: ns3/backoff.h
[ 195/2008] Compiling install-ns3-header: ns3/backoff.h
[ 524/2008] Compiling install-ns3-header: ns3/gplot.h
[ 897/2008] Compiling install-ns3-header: ns3/gplot.h
[1859/2008] Compiling scratch/IPSecPro.cc
[1989/2008] Linking build/scratch/IPSecPro
Waf: Leaving directory `/home/projects/ns-allinone-3.24.1/ns-3.24.1/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (15.136s)
Packet Size without AH1024bytes,Packet Size with AH 1044 bytes and Packet Size w
ithout ESP 5120 bytes Packet Size with ESP 5133 bytes
Could not load icon applets-screenshooter due to missing gnomedesktop Python mod
ule
scanning topology: 50 nodes...
scanning topology: calling graphviz layout
scanning topology: all done.
Enter the length of AES Key(128, 192 or 256 only): 128
55 cb 12a dd 110 ec 103 10f 11f a8 c9 a3 a2 49 b8 124

```

Fig. 12. Snapshot of AES for 128 key size.

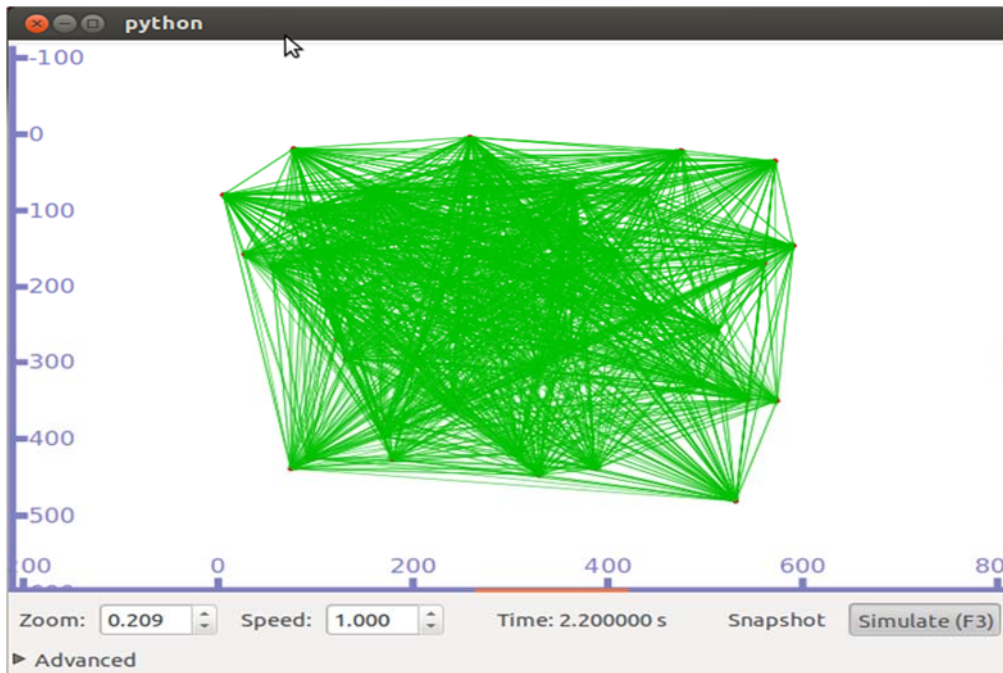


Fig. 13. Simulation of AES for 128 key size.

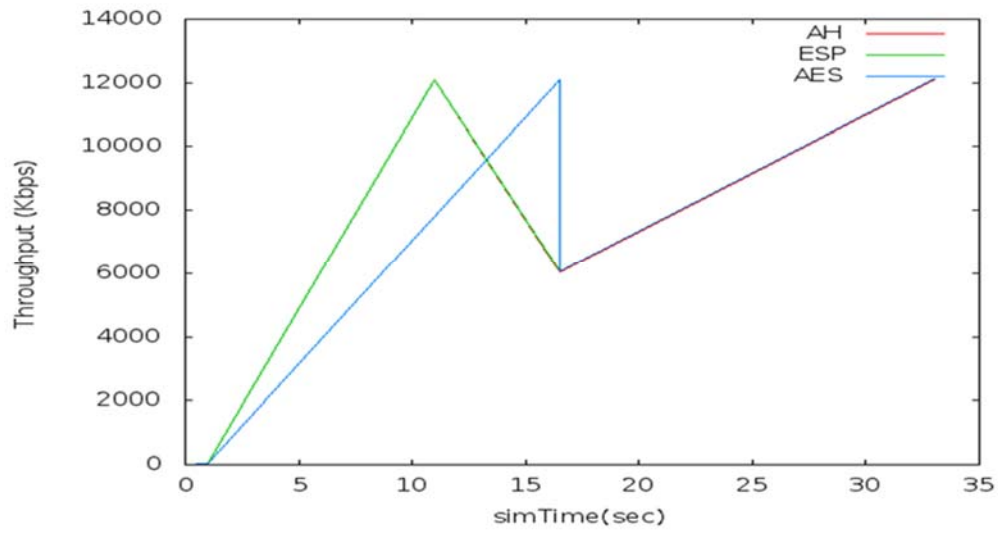


Fig. 14. Results of throughput.

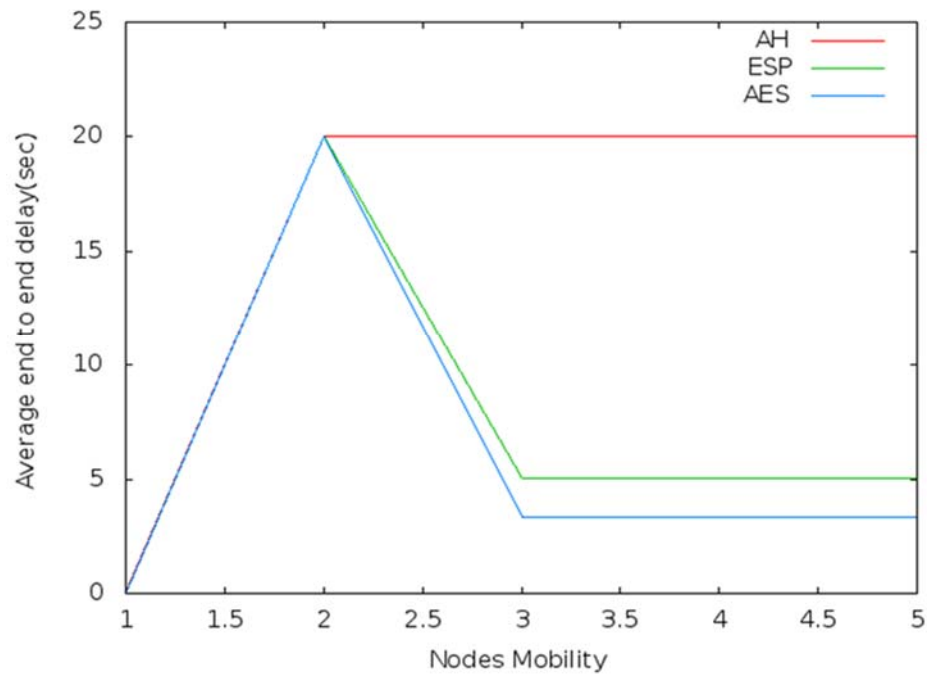


Fig. 15. Results of average End-to-End delay.



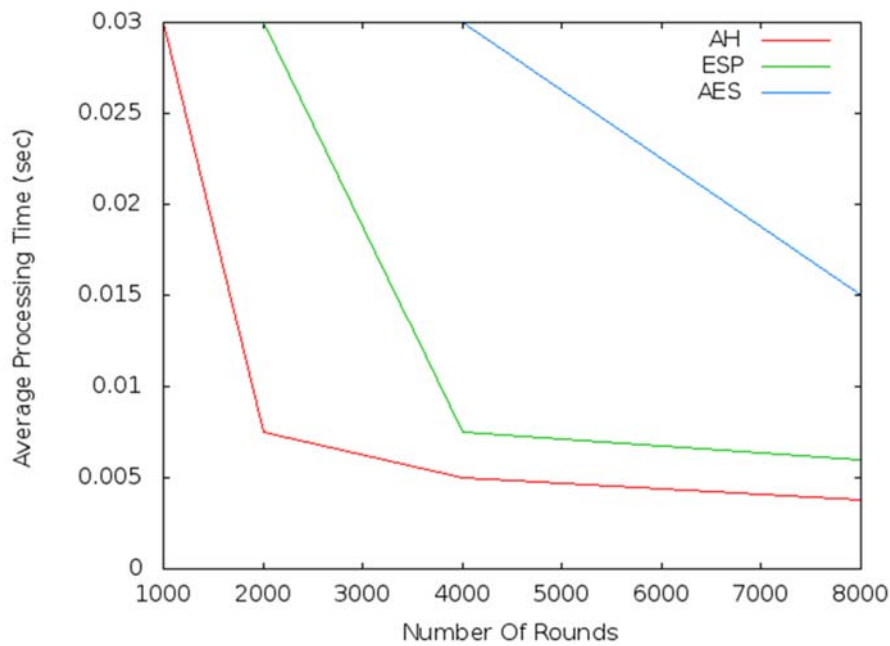


Fig. 16. Results of average processing time.

#### References

- [1] "Ad-Hoc vs Infrastructure Networks What's the difference?" www.usconverters.com
- [2] Ghosh, A., Talpade, R., Elaoud, M. and Berschinsky, M., "Securing Ad-Hoc Networks using IPSec", *IEEE Xplore, Conference: Military Communications Conference, 2005*.
- [3] Helen, D. and Arivazhagan, D., "Applications, Advantages and Challenges of Ad-Hoc Networks", *Journal of Academia and Industrial Research*, 2 (8): 2014
- [4] Kandhil, N. and Kumar, A., "Safe & Secure Data Communication in Mobile Ad-Hoc Network - By Using IPSec Protocol", *IJCSMS International Journal of Computer Science & Management Studies*, 11(01), May 2011.
- [5] Karpjoki, V., "Security in Ad-Hoc Networks", Tik-110.501 Seminar on Network Security, 2000.
- [6] Rahman, F. H. M.A., Thien Wan Au, "Impact of IPSec on MANET", *International Symposium on Computer, Consumer and Control*, 2016.
- [7] Panaousis, E. A., Ramrekha, T. A., Millar, G. P. and Politis, C., "Adaptive and Secure Routing Protocol for Emergency Mobile Ad-Hoc Networks", *International Journal of Wireless and Mobile Networks*, 2(2) 2010.
- [8] Jharbade, N. K. and Shrivastava, R., "Network based Security model using Symmetric Key Cryptography (AES 256- Rijndael Algorithm) with Public Key Exchange Protocol (Diffie-Hellman Key Exchange Protocol)", *IJCSNS International Journal of Computer Science and Network Security*, 12 (8) August 2012.
- [9] Panaousis, E. A., "Security for Mobile Ad-Hoc Networks", *Ph. D. Thesis*, Kingston University, 2012.
- [10] Venkatraman, L., "Secured Routing Protocol for Ad-Hoc Networks", 2000, Special issue on network security, November/December, 1999.
- [11] El Hajjar1, A., Lasebae, A. and Saini, D.K., "Secure routing protocol for Mobile Ad-Hoc Network using IPSec", Conference paper: *WorldCOMP 2012*, At USA, and Volume: ICW-70
- [12] Xenakis, C., Nikolaos Laoutaris, Lazaros Merakos, Ioannis Stavrakakis, "A generic characterization of the overheads imposed by IPSec and associated cryptographic algorithms", *Computer Networks*, 50: 3225-3241(2006).

## محاكاة خوارزميات التشفير في بروتوكول الأمان IPsec أحمد عدس، و عبدالرحمن الشريف

قسم الهندسة الكهربائية وهندسة الحاسبات، كلية الهندسة، جامعة الملك عبدالعزيز، ص.ب ١٠٢٠٤، جدة ٢١٥٨٩، المملكة العربية السعودية

المستخلص. هذه الورقة العلمية تركز على طريقة تأمين انتقال البيانات بين أطراف الشبكة اللاسلكية Ad-Hoc, وذلك من خلال استخدام بروتوكول الأمان IPsec. حالياً، تعتبر شبكات Ad-Hoc أكثر الشبكات انتشاراً واستخداماً في العالم، وأصبح سكان العالم مرتبطين ببعض من خلال هذه الشبكات اللاسلكية باستخدام الهواتف النقالة، التي أصبحت في متناول الجميع، ولكي يستطيع الاتصال بالإنترنت فلا بد من استخدامه للشبكات اللاسلكية. تمكن شبكات Ad-Hoc الأشخاص والأجهزة من الاتصال ببعضهم البعض بدون وجود بنية تحتية معدة مسبقاً للاتصال وبدون مركزية. في بيئة الشبكات اللاسلكية Ad-Hoc نحتاج لتأمين هذه الشبكات خصوصاً أنه كم ذكرنا بأنها ليست لديها مركزية، ولذلك نسبة الأمان في هذه الشبكات ضعيفة، مما جعلنا نبحت ونصل إلى استخدام بروتوكول الأمان IPsec, وتشفيره من خلال استخدام أداة تشفير عالية الجودة، وهي AES "معيار التشفير المتقدم". هناك الكثير من التحديات التي تواجه الباحثين مع الشبكات اللاسلكية Ad-Hoc، منها: الطبوغرافيات الديناميكية بدون وجود قاعدة مركزية، والموجة المعقدة، والمصادر المحدودة، واتصال البيانات الآمن. وتم في هذا البحث تنفيذ بروتوكولات الأمان IPsec وتشفيرها بعمل أداة التشفير AES معيار التشفير المتقدم على الشبكات اللاسلكية Ad-Hoc، كما تمت محاكاة واختبار النظام على برنامج المحاكاة NS-3 لضمان أفضل نظام أمان لهذا النوع من الشبكات.

كلمات مفتاحية: IPsec، AH، ESP، AES، شبكات Ad-Hoc.