The ISC Int'l Journal of Information Security

November 2020, Volume 12, Number 3 (pp. 19–27)

http://www.isecure-journal.org

Selected Paper at the ICCMIT'20 in Athens, Greece

A Hybrid Encryption Algorithm for Mitigating the Effects of Attacks in Ad Hoc Networks**

Abdllkader Esaid [1,*], Mary Agoyi [2], and Muhannad Tahboush [1]

[1] *Department of Computer Engineering, Cyprus International University, Lefkosa, North Cyprus.*

[2] *Information Technology Department, School of Applied Sciences, Cyprus International University, Lefkosa, North Cyprus.*

ARTICLE INFO.

Keywords:
Ad Hoc Network, Security, AODV, Diffie-Hellman, Malicious Node, Intrusion Detection

Type: Research Article

doi: 10.22042/isecure.2021.271065.619

ABSTRACT

Ad hoc network is infrastructure-less support, so network nodes are vulnerable to many attacks. Security attacks in ad hoc networks are increasing significantly with time. The communicated and exchanged data should be also secured and kept confidential. Therefore, a hybrid cryptography is proposed to avoid unauthorized access of data. Data will be transmitted in an encrypted state, through Diffie-Hellman and later decrypted by the intended party. If a third party intercepts the encrypted data, it will be difficult to decipher. Ad hoc on demand distance vector (AODV) routing protocol is employed to determine the destination. The proposed solution is a hybrid mechanism of encryption algorithms. The NS-2.3 simulator was used to evaluate the performance of the proposed security algorithm. Simulation results have shown the performance of the proposed algorithm in ad hoc network on several metrics outperformed many developed security algorithm.

© 2020 ISC. All rights reserved.

1 Introduction

Ad hoc networks are a new paradigm of wireless communication for mobile hosts where node mobility causes frequent changes in topology. Ad hoc networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support movability and organize themselves arbitrarily. This means that the topology of the ad hoc network changes dynamically and unpredictably. Moreover, the ad hoc network can be either constructed or destructed quickly and autonomously without any administrative server or infrastructure. Without support from the fixed infrastructure, it is undoubtedly arduous for people to distinguish the insider and outsider of the wireless network. That is to say, it is not easy for us to tell apart the legal and the illegal participants in wireless systems. Because of the above mentioned properties, the implementation of security infrastructure has become a critical challenge when we design a wireless network system. If nodes of ad hoc networks are mobile and with wireless communication to maintain the connectivity, it is known as mobile ad hoc network (MANET) and require an extremely flexible technology for establishing communications in situations which demand a fully decentralized network without any fixed base stations, such as battlefields, military applications, and other emergency and disas-

* Corresponding author.

**The ICCMIT'20 program committee effort is highly acknowledged for reviewing this paper.

Email addresses: aawatas2@gmail.com, magoyi@ciu.edu.tr, mh_tahboosh@yahoo.com

ISSN: 2008-2045 © 2020 ISC. All rights reserved.

ter situations. Since, all nodes are mobile, the network topology of a MANET is generally dynamic and may change frequently. Thus, protocol such as 802.11 to communicate via same frequency or Bluetooth have require power consumption is directly proportional to the distance between hosts, direct *single-hop* transmissions between two hosts can require significant power, causing interference with other such transmissions. To avoid this routing problem, two hosts can use *multi-hop* transmission to communicate via other hosts in the network. A router should provide the ability to rank routing information sources from most trustworthy to least trustworthy and to accept routing information about any particular destination from the most trustworthy sources first. A router should provide a mechanism to filter out obviously invalid routes. Routers must not by default redistributes routing data they do not themselves use, trust or otherwise consider valid. Routers must be at least a little paranoid about accepting routing data from anyone, and must be especially careful when they distribute routing information provided to them by another party.
As ad hoc networking somewhat varies from the more traditional approaches, the security aspects that are valid in the networks of the past are not fully applicable in ad hoc networks. While the basic security requirements such as confidentiality and authenticity remain, the ad hoc networking approach somewhat restricts the set of feasible security mechanisms to be used, as the level of security and on the other hand performance are always somewhat related to each other. The performance of nodes in ad hoc networks is critical, since the amount of available power for excessive calculation and radio transmission are constrained, as discussed e.g. in [1]. In addition, the available bandwidth and radio frequencies may be heavily restricted and may vary rapidly. Finally, as the amount of available memory and CPU power is typically small, the implementation of strong protection for ad hoc networks is non-trivial.

2 Security Issues in Ad Hoc Networks

Use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion eavesdropping might give an attacker access to secret information thus violating confidentiality. Active attacks could range from deleting messages, injecting erroneous messages; impersonate a node etc. Thus violating availability, integrity, authentication and non-repudiation. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised.

2.1 Availability

Ensure availability of network services in the context of various attacks in the environment. Availability is mainly concerned with the resources, which can heal the network services immediately [2]. Some attacks have programmed counteragent such as encryption and authentication, whereas some attack requires different sort of actions to limit or get back from loss in the availability services.

2.2 Confidentiality

Confidentiality ensures that data is only available by the relying party. Protect data from attacks [3].

2.3 Integrity

Integrity ensures that it is granted only to parties authorized to change information or messages. It also protects the message, because the transmission does not get any damage. Integrity services apply to any type of message, whether message flow, message, or fields specified in the message [4].

2.4 Authentication

Authentication verifies with soothe that a link is accurate [5]. Without authentication, malicious node will try to gain illegal access to reserves and sensitive information, and also tries to agitate the operations of the other nodes [6].

2.5 Non-repudiation

Non-rejection places an end to the sender or recipient to oppose a sent message (Sogani and Jain, 2015). Therefore, when a message is delivered, the destination node can prove that the data was sent by the intended sender and vice versa [7].

2.6 Scalability

Scalability is very important aspect on safety account. An MANET is abiding of large numbers of nodes. Potential security must be manageable in managing large networks. Otherwise, the attacker maliciously uses the fresh added node in the network and will use it to approach the entire system [5].

2.7 Anonymity

In this, all the data that is used to identify the authorized user of node, they must be stored confidential and must not be assigned to the same node or structure [6].

3 Attacks on Ad Hoc Network

Ad hoc networks can be subjected to various types of attacks. They can be summarized as follows:

3.1 Black Hole

In this type of attack, the malicious node injects fake route replies to the route requests it receives, advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

3.2 Wormhole

The wormhole attack involves the cooperation between two malicious nodes that participate in the network. One node of the attackers will capture routing traffic at one point of the network and tunnels them to another node in the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers [8].

3.3 Location Disclosure

Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques, or with simpler probing and monitoring approaches, where the attacker can discover the location of a node, or even the structure of the entire network.

3.4 Denial of Service

Denial of service attacks can cause a complete disruption of the routing function and affects the whole operation of the ad hoc network. Some of these examples of the denial of service attacks are the routing table overflow and the sleep deprivation torture. Where in a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes [9].

3.5 Blackmail

This attack affects the routing protocols that based on some mechanisms to identify the malicious nodes and propagate the messages that try to blacklist the offender. An attacker will use these reporting messages by fabricating them and try to isolate these legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated [10].

3.6 Rushing Attack

Rushing attack is that results in denial of service when used against all previous on-demand ad hoc network routing protocols (e.g. AODV, DSR), and security protocols which are based on them, like SAODV, Ariadne, and can't discover routes longer than two hops when they are subjected to this attack. To develop rushing attack prevention, that allow that protocol to resist the rushing attack, a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol [11, 12].

3.7 Breaking the Neighbor Relationship

In this attack, an intelligent filter is placed on a communication link between two information system by the intruder to change or modify the information in the routing updates or may be to intercept traffic belonging to any data session [13, 14].

3.8 Masquerading

During the acquisition process between neighbors, an outsider intruders could masquerade as nonexistent or existing information systems by attaching themselves to communication link and illegally try to join the routing protocol domain by compromising authentication system [15, 16].

3.9 Routing Table Poisoning

The routing tables and related routing information for the network are usually maintained by the routing protocols. In routing table poising attack, a fabricated traffic signal will be generated and sent by the malicious nodes. Or these nodes can modify legitimate messages from other nodes to produce a false entries on the participating nodes. Routing table poisoning attacks may cause creation of routing loops, bottlenecks, and selection of non-optimal routes [9].

3.10 Passive Listening and Traffic Analysis

The intruder can passively gather the exposed routing information. This type of attack cannot affect the operation of routing protocol, but it is a breach of user trust to routing the protocol [17].

3.11 Replay

An attacker that performs a replay attack injects into the network routing traffic that has been captured

previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions [18].

4 An Overview of Cryptographic Techniques

It is a difficult decision to make which cryptographic techniques should be used, how often they are used, which network performance metrics are used to evaluate the design, and security analysis. The first choice may be when the designer should use symmetric cryptography and when should the designer use asymmetric cryptography? For example, in order to get better performance, a hash key chain can sometimes be a better choice than an asymmetric private key for encryption due to MANETs' and WSNs' dynamic changes. Specifically, alternative temporary symmetric secret keys may be better than asymmetric 1024 bit public keys.

4.1 Advanced Encryption Standard

Advanced encryption standard (AES) is considered a new block cipher which also acts as a new replacement for data encryption standard (DES). AES uses 128-bit blocks with only having three types of encryptions keys that are 128-bit, 192-bit, and 256-bit. AES uses several rounds in which each round is made of several stages. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size. It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications. To provide security AES uses kinds of transformation. Substitution permutation, combination and key adding every round of AES accept the last uses the four transformations. A modification for the AES is proposed to increase its efficiency and its security by adjusting the shift row transformation. Instead of the initial shift row, a tendency to modify it by examining the value within the initial row and initial column, (state [0][0]) whether it is even or odd. If it's odd, the shift rows step operates on the rows of the state; it cyclically shifts the bytes in every row by a particular offset [19]. For modified advanced encryption standard (MAES), the primary and third rows are unchanged and every computer memory unit of the second row is shifted one to the left. Similarly, the fourth row is shifted by three to the left. Rows step operates on the rows of the state; it cyclically shifts the bytes in every row by an exact offset. The initial and fourth rows area unit unchanged and every computer memory [20].

4.2 Blowfish Security Algorithm

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. Blowfish can be efficiently used for encryption and protection of facts and it is a Symmetric Block Cipher (SBC) [21]. Blowfish is ideal for securing statistics, takes a variable key usually from 32-48 bits. Blowfish set of rules, iterating a simple encryption feature 16 instances. Blowfish designed in 1993 by Bruce Schneider as a firm, open alternate to present encryption set of rules. The algorithm consists of two Parts: a key-expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent Permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round [22].

4.3 Diffie-Hellman

Diffie-Hellman algorithm is an asymmetric algorithm used to establish a shared secret for a symmetric key algorithm. Nowadays, most of the people uses hybrid crypto system i.e., combination of symmetric and asymmetric encryption. Asymmetric Encryption is used as a technique in key exchange mechanism to share secret key and after the key is shared between sender and receiver, the communication will take place using symmetric encryption. The shared secret key will be used to encrypt the communication. Some systems were proposed type in which two parties communicating solely over a public channel and using only publicly known techniques that can create a secure connection which is based on Diffe-Hellman key exchange [23].

5 Proposed Security Algorithm

Ad hoc network is infrastructure-less support, so network nodes are vulnerable to many attacks. Security attacks ad hoc network are increasing significantly with time. The communicated and exchanged data should be also secured and kept confidential. Therefore, hybrid cryptography is the technique used to avoid unauthorized access of data. Data will be transmitted in an encrypted state, through DH and later decrypted by the intended party. If a third party intercepts the encrypted data, it will be difficult to decipher. The security of modern cryptosystems is not based on the secrecy of the algorithm, but on the created secure channel that pass the information through. The fundamental and classical task of cryptography is to provide confidentiality by encryption methods. The proposed algorithm is based in standard security algorithms to protect any ad hoc network. Where a hybrid of these standard algorithms are manipulated to develop the proposed algorithm. The algorithm proposes an encryption from the source node to the re-

quired destination node. In the node encryption part from the sender node side, the following standard algorithms and steps are proposed to encrypt the data.

Transmitter side algorithm:

A. Take plain text message and use it as input message
B. Apply (MAES) as first encryption method
C. Apply (Blowfish) as second encryption method
D. Apply Diffie-Hellman for securely exchanging cryptographic keys over a public channel through generating public key for sender and private key for receiver for two pairs on sides
E. Using AODV reactive routing protocol to detect the trusted node to determine the location of the destination node and send route request RREQ.

Receiver side algorithm: While at the destination node where the data will be decrypted as follows:

A. The encrypted message as input message
B. Decrypt the encrypted message that encrypted using (MAES) private key
C. Decrypt the encrypted message that encrypted using (Blowfish) private key
D. Verify the Diffie-Hellman key at the destination side
E. Reply with route reply RREP to the source node. The complete algorithm is shown for encryption and decryption mechanisms in Figure 1

6 Proposed Algorithm: Implementation and Results

The proposed algorithm consists of a hybrid of standard encryption techniques where some of them are symmetric and the others are asymmetric which forms a hybrid framework for encryption and decryption of data. The data will be transmitted from the source node to a destination node using the data encryption mechanism and the destination will use the data decryption mechanism to restore the data. The implementation process is conducted using three scenarios each has different number of nodes, 50, 75, and 100 nodes are susumed for the scenarios. Different matrics are employeed to evaluate the performance of the proposed algorithm like packet drop ratio, throughput, power consumption, and delay.

6.1 Performance Evaluation of the Proposed Algorithm

To evaluate the performance of detection method and accuracy of the proposed algorithm. It has been simulated using NS-2 simulator environment on Ubuntu 16.04 LTS operating system. Then, the proposed algorithm tested under particular parameters which make

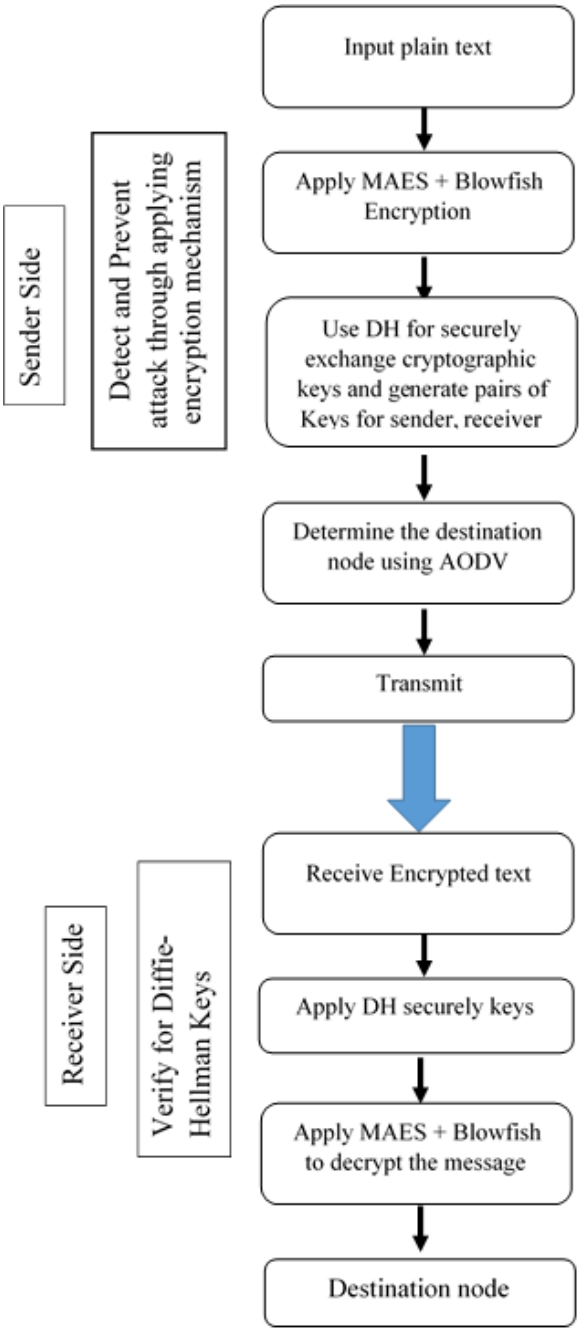

Figure 1. Flowchart for the proposed algorithm

the system perform best. Table 1 shows the simulation parameters that are considered during the simulation environment. To compare the performance of the proposed algorithm with other developed algorithms, a simulation also is carried out for the selected research work which is considered as a base approach for comparison [24].

6.1.1 Throughput

One of the most important measures to evaluate the performance of any security algorithm is throughput

Table 1. Parameters list for proposed algorithm simulation

Parameter	Value
Simulator	NS-2.3/ Ubuntu 16.04 LTS
Topological area	500 m x 500 m
Simulation time	500 seconds
Node locations	Randomly
Radio propagation model	Two-ray ground reflection
Mobility model	Way point
Traffic type	CBR
Packet size	512 bytes
Number of nodes	50,75, 100 nodes
Protocol	AODV
Channel Type	Wireless

which indicates the amount of packets received at the destination side in one second. Throughput measures how many packets arrive at their destinations successfully. For the most part, throughput capacity is measured in bits per second, but it can also be measured in data per second. Packet arrival is key to high-performance service within a network. It is effected with security attacks that ensure the arrival of packets. The proposed algorithm has shown better performance over the base approach since it has achieved more values for throughput for three scenarios (50, 75, 100 nodes) as shown in Table 2 and in Figure 2.

Table 2. Obtained values for throughput

No. of Nodes	Base Approach	Proposed Approach
50	2641.91	3112.5
75	2459.12	2945.1
100	2390.1	2840.4

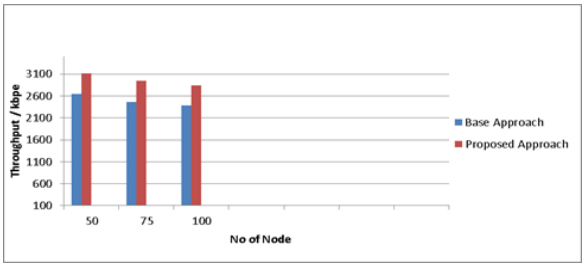

Figure 2. Comparison between the proposed algorithm and Base [24] from throughput perspective

6.1.2 Delay

Security protocols are featuring delay tolerance and energy efficiency for large WSNs in the security application domain since connections among nodes are dynamically established according to physical location of the nodes. In security-critical applications, the deployment of large networks faces difficulties among othersthe implications of delay variability on the correct operation of security algorithms. Many security protocols featuring delay tolerance and energy efficiency for large WSNs in the security application domain. The proposed algorithm has been tested to measure the delay in data transmission from the source node to the destination. The proposed algorithm has shown better performance over the base approach since it has witnessed less delay by implementing the three scenarios, where almost half of the time is needed for data transmission w in the different number of node density. The values are shown in Table 3 and in Figure 3.

Table 3. Obtained values for packet ratio

Number of Nodes	Base Approach	Proposed Approach
50	83.79	48.9
75	90.1	52.5
100	93.8	57.1

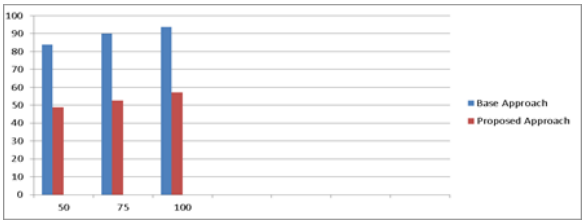

Figure 3. Comparison between the proposed algorithm and Base [24] from delay perspective

6.1.3 Packet Delivery Ratio

The packet delivery ratio can be obtained from the total number of data packets arrived at destinations divided by the total data packets sent from sources. In other words Packet delivery ratio is the ratio of number of packets received at the destination to the number of packets sent from the source. The proposed algorithm has shown improvement in the ratio of packet delivery in the three different scenarios as shown in Table 4 and in Figure 4.

Table 4. Obtained results for packet delivery ratio

Number of Nodes	Base Approach	Propose Approach
50	57.96	72.3
75	52.3	68.9
100	47.9	63.3

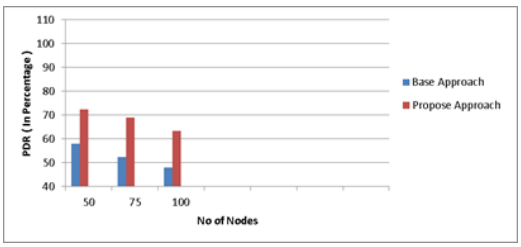

Figure 4. Comparison between the proposed algorithm and Base [24] from packet delivery ratio perspective

6.1.4 Packet Dropping Ratio

A path between a source node and a destination node in a MANET is established using a route discovery process. Once this has been done, the source node starts sending the data packet to the next node along the path; this intermediate node identifies the next hop node towards the destination along the established path and forwards the data packet to it. This process continues until the data packet reaches the destination node. To achieve the desired operation of a MANET, it is important that intermediate nodes forward data packets for any and all source nodes. However, a malicious node might decide to drop these packets instead of forwarding them; this is known as a data packet dropping attack, or data forwarding misbehavior. In comparison to deliberately malicious behavior, in some cases nodes are unable to forward data packets because they are overloaded or have low battery reserves; alternatively the nodes may be selfish, for example saving their battery in order to process their own operations. Packet dropping attacks differ from black hole and grey hole attacks (see below) because there is no attempt to capture the routes in the network.

In ad hoc networks that does not have any black hole, the information traffic could be dense and packets would possibly get lost. The proposed algorithm dropping ratio has shown less ratio than the base approach dropping ration in three different scenarios as shown in Table 5 and Figure 5.

Table 5. Obtained results for packet dropped ratio

Nodes	Base Approach	Proposed Approach
50	42.04	27.7
75	47.7	31.1
100	52.1	36.7

6.2 Consumed Energy

The design of routing protocol with energy efficiency and security is a challenging task. To overcome this challenge, the proposed security algorithm is considered as energy-efficient. Figure 3 shows the total energy consumed in the ad hoc network with varying number of nodes. The number of connections is taken as 50% of the number of nodes in the network and the nodes are moving at speed of 10m/sec with pause time of 0 seconds. Figure 6 gives the variation of total energy consumed with number of connections in a network with 50 nodes. It is clearly seen that the proposed algorithm outperforms the base approach as the load in the network increases as shown in Table 6. The energy consumption in the network is reduced by 10%-20% in the proposed algorithm in comparison with the based approach.

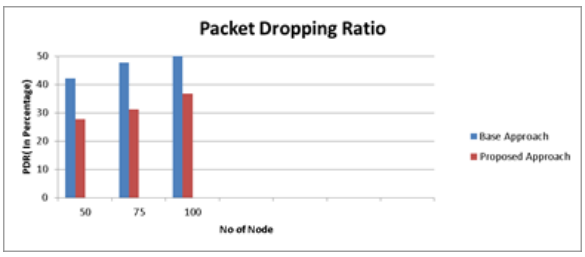

Figure 5. Comparison between the proposed algorithm and Base [24] from packet dropping ratio perspective

Table 6. obtained values for consumed energy

Nodes	Base Approach	Proposed Approach
50	53.9	45.1
75	60.1	55.5
100	68.3	60

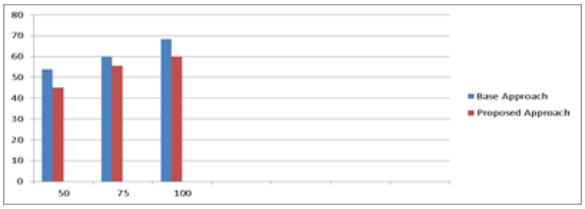

Figure 6. Comparison between the proposed algorithm and Base [24] from packet dropping ratio perspective

7 Conclusion

A hybrid encryption algorithm for mitigating the effects of attacks in ad hoc networks was developed based on ADOV routing protocol. The algorithm manipulated AES and Blowfish encryption algorithms to increase the speed of the algorithm as well as encryption which will lead to prevent access to packet while transmission in ad hoc network. In addition, Diffie-Hellman key exchange is used to provide exchanging cryptographic keys over a public channel or insecure network. The proposed algorithm was simulated by using NS2 simulator and it has shown a high performance in various metrics compared with others.

References

[1] R Shiva Kumaran, Rama Shankar Yadav, and Karan Singh. Multihop wireless lan. *HIT haldia March*, 2007.

[2] Vishal Kumar Sagtani and Sandeep Kumar. Modern approach to enhance routing recitation in manet. *International Journal of Emerging Technology and Advanced Engineering*, 4(7):265–270, 2014.

[3] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani. A survey of secure mobile ad hoc routing protocols. *IEEE communications surveys & tutorials*, 10(4):78–93, 2008.

[4] Monika Goyal, Sandeep Kumar Poonia, and Deepak Goyal. Attacks finding and prevention techniques in manet: a survey. *Adv Wireless Mob Commun*, 10(5):1185–1195, 2017.

[5] Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, and Benachir El Hadadi. Secure routing protocols for mobile ad hoc networks. In *2016 international conference on information technology for organizations development (IT4OD)*, pages 1–7. IEEE, 2016.

[6] Ana Lucila Sandoval Orozco, Julián García Matesanz, Luis Javier García Villalba, José Duván Márquez Díaz, and T-H Kim. Security issues in mobile ad hoc networks. *International Journal of Distributed Sensor Networks*, 8(11):818054, 2012.

[7] Priyanka Sogani and Dr Aman Jain. A study on security issues in mobile ad hoc networks. *IJIACS ISSN*, pages 2347–8616, 2015.

[8] Y-C Hu, Adrian Perrig, and David B Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428)*, volume 3, pages 1976–1986. IEEE, 2003.

[9] Imad Aad, Jean-Pierre Hubaux, and Edward W Knightly. Denial of service resilience in ad hoc networks. In *Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 202–215, 2004.

[10] Patroklos G Argyroudis and Donal O'mahony. Secure routing for mobile ad hoc networks. *IEEE Commun. Surv. Tutorials*, 7(1-4):2–21, 2005.

[11] Junghyun Nam, Seokhyang Cho, Seungjoo Kim, and Dongho Won. Simple and efficient group key agreement based on factoring. In *International Conference on Computational Science and Its Applications*, pages 645–654. Springer, 2004.

[12] Yih-Chun Hu, Adrian Perrig, and David B Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proceedings of the 2nd ACM workshop on Wireless security*, pages 30–40, 2003.

[13] Charles Perkins and E. Royer. The ad hoc on-demand distance-vector protocol. In *Ad Hoc Networking*, page 173219. Addison-Wesley, 2001.

[14] Jim Parker, John Pinkston, Anupam Joshi, et al. On intrusion detection in mobile ad hoc networks. In *23rd IEEE International Performance Computing and Communications Conference–Workshop on Information Assurance*, 2004.

[15] S Sarika, A Pravin, A Vijayakumar, and K Selvamani. Security issues in mobile ad hoc networks. *Procedia Computer Science*, 92:329–335, 2016.

[16] Jeremy J Blum and Azim Eskandarian. A reliable link-layer protocol for robust and scalable intervehicle communications. *IEEE Transactions on Intelligent Transportation Systems*, 8(1):4–13, 2007.

[17] Jung-San Lee and Chin-Chen Chang. Secure communications for cluster-based ad hoc networks using node identities. *Journal of Network and Computer Applications*, 30(4):1377–1396, 2007.

[18] Yuh-Ren Tsai and Shiuh-Jeng Wang. Routing security and authentication mechanism for mobile ad hoc networks. In *IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004*, volume 7, pages 4716–4720. IEEE, 2004.

[19] Joan Daemen and Vincent Rijmen. *The design of Rijndael*, volume 2. Springer, 2002.

[20] AkoMuhamad Abdullah. Advanced encryption standard (aes) algorithm to encrypt and decrypt data. *Cryptography and Network Security*, 16, 2017.

[21] G Manikandan, N Sairam, and M Kamarasan. A new approach for improving data security using iterative blowfish algorithm. *Research Journal of Applied Sciences, Engineering and Technology*, 4(6):603–607, 2012.

[22] B. Schneier. *Applied Cryptography*. John Wiley & Sons, New York, 1994.

[23] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[24] Hiral Vegda and Nimesh Modi. Secure and efficient approach to prevent ad hoc network attacks using intrusion detection system. In *2018 Second international conference on intelligent computing and control systems (ICICCS)*, pages 129–133. IEEE, 2018.

Abdllkader Esaid received the master's degree in information technology from University TUN Abdulrazak, Malaysia, in 2010. He is currently pursuing the Ph.D. degree in computer engineering with Cyprus International University, Nicosia, and

North Cyprus. His research interests include network security, and data communication.

Mary Agoyi received the Ph.D. degree in computer engineering. She is currently an assistant professor with Cyprus International University. Her research interests include networking, information security, and image watermarking.

Muhannad Tahboush was born in Amman, Jordan. He received the bachelor's degree in computer engineering from Near East University, North Cyprus, in 2003, and the master's degree in computer science from DePaul University, in 2008. He is currently pursuing the Ph.D. degree in computer engineering with Cyprus International University, Nicosia, North Cyprus. His research interests include network security, cryptography, and data communication.