Trustworthy Position Based Routing to Mitigate against the Malicious Attacks to Signifies Secured Data Packet using Geographic Routing Protocol in MANET

SUDHAKAR SENGAN[1], S.CHENTHUR PANDIAN[2]

[1]Research Scholar, Anna University, Chennai, Tamilnadu, India.

Email:sudhakarsengan@gmail.com

[2]Principal,S.N.S. College of Technology,Coimbatore, Tamilnadu, India.

Email:chenthur@rediffmail.com

*Abstract:-*A mobile ad hoc network (MANET) is a dynamic wireless network that can be formed without the need for any pre-existing infrastructure in which each node can act as a router. Instead of using topology based routing protocolto prefer Geographic Routing Protocol (GRP) become scalability and to improve more successive rate and also reducing the overhead. Here proposed a novel secure position-based routing protocol, it takes dynamic pseudo identifiers instead of its real identity in advertising its position. Though the MANET hasdifferent malicious attacks such as flooding, black hole and wormhole etc.because of simulation studies demonstrate that the networks with 15% malicious nodes show significant performance degradation. To present secure communication and transmitting recommended that this tactics is actually asymmetric encryption technique. Simulation is focused to take measurements in the light of throughput, end-to-end delay and network load and using this modified asymmetric cryptographic technique's to improve the through put and reduced the packet drop against malicious attacks.

Keywords: -MANET, Geographic Routing Protocols, Cryptography, Performance, Malicious Attacks.

1. Introduction

Ad hoc networks consist of mobile or immobile nodes that connect over wireless links. There is neither predetermined infrastructure to support the transmission nor any directed operations or standard support services. Nodes can self-organize dynamically in randomly and short-term manner allowing people and devices to gracefully communicate in areas with no Pre-existing communication infrastructure; Thus, the particular nodes by themselves represent routers likewise. In addition, owing to the confined indication range of wireless nodes, sophisticated nodes may be required to work together in forwarding a packet from source to destination. Thus, nodes outside strong wireless transmitting array of one another can connect by using multi-hop routing. The emphasis in this report is especially on Mobile Ad Hoc Networks (MANETs), the spot that the redirecting activity gets to be more strenuous due to nodes' flexibility. In truth, powerful topology adjustments are among the attributes regarding mobile ad hoc sites wherever nodes transfer often. Thus, many of us can't depend upon classic redirecting standards made for born networks with the intent of redirecting in MANETs. Since, because numerous fresh routing standards regarding mobile random systems are generally examined and also created. Some of them, under the category of geographic routing are discussed in this paper. There are different cases and situations where MANETs are employed; some of them include: military battlefields, catastrophe recovery and emergency shelter expeditions, Vehicle Ad Hoc Networks [1].

One way of communication in these kinds of networks might appear to be simply avalanche the entire network. However, the reality that energy and data transfer used tobeavoiding resources in such networks of low powered wireless devices demands more successful routing protocols. Therefore, there are a variety of routing protocols proposed for MANETs, which can be categorized into two different strategies: topology-based and position-based routing [2].

Topology-based routing protocols use route preservation, path establishment dependent of the network links. Most of these methodologies is divided into proactive, reactive and also hybrid procedures. Dynamic Source Distance Vector (DSDV), Open Link State Routing (OLSR) is illustrations of proactive routing. Dynamic Source Routing (DSR) [4] and Ad-Hoc On-Demand Distance Vector Routing (AODV) [3] are usually are cases involving reactive methods. An illustration of a hybrid routing protocol is Zone Routing Protocol (ZRP) [5].In circumstance of topology changes, which result in link problems, route error communications are made. Despite the fact that this will be only executed for the routes in use, the issue of impacting on traffic at times of topology changes is not solved absolutely. A survey and assessment of topology based protocols can be found in [6, 7].

Unique tactics used in direction-finding technique throughout ad hoc sites include the position-based direction-finding methods that are have to have and keep tracks for you to destinations. These types of routing methodologies use the geographic position measurable on the nodes to complete packet forwarding. Every node is helpsto determine a geographic position such as GPS or additional kind of location establishments. A position-based direction-finding strategy which is used as a confidence to eliminatemany restrictions with regards to topology based direction-finding by making use of more details. Theyrequire information in regards to the physical position from the participating nodes. The redirecting selections with each and every node are usually and then while using destination's position included and also the position of the forwarding node's neighbors. Therefore position-based direction-finding is not going to need the private along with mend affecting routes. These nodes should have routing tables andthey have to transfer emails to hold routing table's up-to time frame. Any position-based standard protocol involves a pair of major techniques to send out the packet involving the nodes in network.

Position-based or geographic routing techniques were announced to remove some of the limits of the topology-based protocols in MANETs. These routing protocols are dependent on having one part of information that is the nodes' authentic position information and facts. Thus, it is essential for nodes to attain harmonizes frequently by using a location service such as GPS or other kinds of location services [8, 9]. A review of these services can be found in [10]. By making use of position information, geographic routing protocols do not need to set up and preserve routes, thereby minimizing routing table building and preservation. In this survey, we pertain to position-based routing protocols frequently as geographic routing. The forwarding strategy in these protocols is based on location information of the destination as well as the one hop neighbours. The forwarding method cannot work when there is no one-hop neighbors whose place is closer to desired destination compared to the forwarding node. Within these types of access tactics are usually presented to handle thesetypes of troubles. An evaluation of topology-based redirecting methodologies (AODV, DSR [11, 12]) in addition to Greedy-Perimeter Stateless Routing protocol (GPSR) can be presented exemplar, without having the particular methodologies facts. Within period efficient information and delivery along with several cost position-based protocols are more advanced than their topology-based counterparts. In addition, the results provide how the direction-finding techniques will not employ geographic position on the inside direction-finding selections aren't scalable. The issues about transmit storm troubles in topology-based methodsand it shows in Figure 1 and 2.

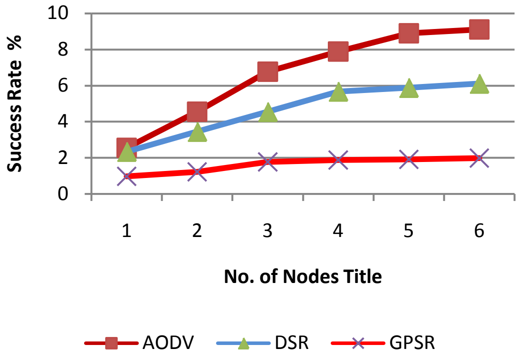


Figure 1. Success rate of position-based and topology-based redirecting process.

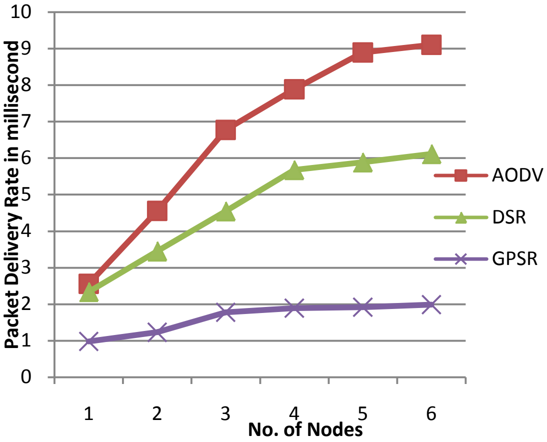


Figure 1. Route over head of position-based and topology-based redirecting process.

The fact is that, in the position-based routing protocols, every single node has to routinely promote/share its current position to all its one-hop neighbors. Such coverage of position information can direct to catastrophic effects in some applications with a robust need on user location privacy. Allow to consider the request of the battle field as an example. Each soldier and commander could carry mobile devices, which are dynamically associated together to form a MANET. If a node persists broadcasting its position information and network identifier, an adversary is able to discover its real identifier and location if information transmitted over the network is not secured. Even worse, the opponent can identify the essential nodes or end users based on the sniffed details. Even if the real identity of nodes is undetectable, an attacker can still identify the essential nodes through network traffic analysis. Of course, after locating the essential nodes, the attacker may launch a Decapitation effecton individual's essential nodes to win the battle rapidly [13]. In addition to battlefield use, the privacy prerequisite on actual physical locations can be attended to in some other professional applications. As a result, it is critical to equip a routing with the knowledge of location level of privacy for every single node in the MANET.

MANETs have some kind of protected opportunity for indication and communication. And this is the challenging and necessary issue since there is certain improvements provocations regarding attack on the mobile networks. Safeness would be the weep with the time. As a way to produce protected verbal exchanges as well as transmitting, the technicians must recognize unique variations of attacks as well as the effects in MANETs.Black hole attack, Wormhole attack, flooding attack, Sybil attack, routing table flood attack, Denial of Service (DoS), and self-centered node performing unnecessarily.Impersonation attacks usually are form of assaults a MANET may experience via. The MANET is faced such problems since relationship is founded on common misbehave amongthe nodes; there isnot a key point for central administration, absolutely no authorization middle, purposely adjusting topology along with confined solutions.

Due to malicious attacks, an information security technique is applied for secure communication. These information securities will be attained via using cryptographic algorithms as like DES, AES, Blow Fish and many others. AES [16] may be the Advanced Encryption Standard algorithm FIPS-197 that has been applied considering the fact that 2001 and it also provides substantial quantity security and can end up being included simply. This AES is really a symmetric cipher algorithm having block size with 128-bit makes it possible for key dimensions connected with 128, 192, and also 256 parts having 10, 12, or 15 version rounds, keeping that in mind. Four significant procedures are done for the duration of each round: byte substitution, shifting rows, mixing columns, and as a final point adding the round key. AES 128 bit key is deemed secure as opposed to the other existing symmetric cipher algorithms. It is extensively used in numerous applications where the security is a significant. The new variable AES algorithm produces seven additional securities and twice the throughput. More security occurs from working with variable key size, and more throughput's are available from using more times variable block size than the block size used in the primary AES. The only weakness of variable AES is the need for more pattern area. The recommended variable AES algorithm has four main several byte-based transformations. The initial transformation is the Byte Substitution which substitutes the several bit values and this is accomplished via using comparative S-boxes. The subsequent transformation is Shifting Rows that shift the rows of the output from the earlier step by a countered equals to the row number. The next transformation is Mixing Columns, where each column of the result from the earlier step is increased by several values. The last transformation in the round is Adding the Round Key to the remaining result of this round.

In this specific paper, will probably exchange about utilization of node's location details intended for redirecting requirements. And confirm the security assurance as well as privacy-preservation from the proposed plan, some probability product can be developed with the monitoring attack under GRP. Significant simulations usually are conducted to show this success and effectiveness from the GRP program, where equivalent functionality is usually seen with that by GRP as you move the place privacy is typically maintained. Within this paper, the scheme for your diagnosis involving approved nodes then selecting overseeing nodes in MANETs. This can identify the primary network characteristics with network covering and also link layer. The primary step is founded on absolutely no understanding technique which usually doesn't count on your algorithms regarding symmetric as well as asymmetric encryption, electronic digital signatures, sequence numbers and time imprints to distinguish nodes. This method will depend on evidence. So, the actual recommended technique works extremely well in MANET Attackers. Further a new fresh trustworthy pertaining to position-based answer pertaining to high quality involving support (QoS) redirecting throughout mobile ad hoc sites can be proposed. The intention of this study should be to found the actual variable AES for being employed as soon as larger examples of security and also throughput are usually demanded devoid of rising the full design spot as soon as in contrast while using the key Rijndael criteria. The amount associated with process functionality along with challenging calculation provided by protection components, in which report discloses a commitment intended for realizing Quality of Service (QoS) and various protection intended for putting into action, the performance method by applying variable AES.The new algorithm has identical framework to the primary AES with variable plaintext size and key size.

2. Related Studies

2.1. Position Based Routing

In typically, redirecting methods might be classified in to a couple of broad different types: topology based in addition to location based forwarding methods [17] [18]. Specifically, topology structured approaches are generally labeled into a couple subcategories: reactive as well as proactive, make use of information for forwarding the precise packets involving nodes on the community. Well known methodologies with the essential types tend to be AODV, as well as DSR. In position-based routing protocol, the particular routing determination just isn't predisposed by a routing dining room table yet at each node; the particular routing last decision is based upon the particular positions which are nearby nodes as well as the destination node.

Though studies have been unveiled while assessing the general efficiency regarding routing methods used with numerous ability to move versions, and various traffic consequence's situations along with diverse proficiency metrics.Lochert et al [19] weighed against numerous routings are generally AODV, DSR, along with Geographic Source Routing (GSR).The item demonstrates GSR which in turn mixes both equally position-based routing having topological problems regarded overhead can be taken place topological expertise outperforms with regard to primarily in both AODV and DSR having worth for you to delivery rates and also latency.

In Position based routing (LAR) is explained [20] to lessen the routing overhead with the utilization of position information. It's largely for restricting the overflows to some particular location called demand zone. Experts in addition found that LAR is a lot better pertaining to VANET platforms. Position dependent routing protocols [21, 22] need to have the information about the actual location of participating vehicles be available for using position oriented purposes. This position can be obtained periodically by the transmitted control messages or beacons to the direct neighbors. When the sender can request the position of a receiver. Later the vehicular nodes are seen to proceed with founded routes plus routing tables.

Comparing with GSR, GPSR [23, 24] is a node detects the location of its neighbors by implies of their HELLO messages and the position of destination to get the help of a location service. GPSR involves that every node in the network is able to discover its present position by making use of GPS receiver which provides current location, speed, current time and direction of the vehicles. A node forwards inward packets to a neighbouring node closest to the destination, which is located in a geographical region. This operating mode is known as Greedy Forwarding in which the neighboris closest to the destination and that is to be selected as the next-hop node.

2.2. MANET Attacks

MANET, which is active, facilities fewer and scalable. Despite MANET, most of these networks are a good deal which is ready to accept problems [25, 26].Wireless links also creates the problem in MANET which is more vulnerable to attacks. And it is moredifficult to enter into network to obtainconstanttransmission [25, 27] standards can also be staying tapped throughout flooding attack, by using RREQ or even data flooding techniques[29].Though various types of attacks are already investigated in MANET. Gray hole attacks is one type of attack that acts as malicious node until the packets fallen and transformtheir common behavior [28].

In different system, the data must be secure, tactic without necessity involving aggressive steals. Fairly a few attackers think separately to offer the least level bandwidth as well as higher bandwidth made available for the indication including throughout wormhole attack, and also the opponent gets themselves support throughout the network. Theygeneratenode for their precise location to get the shortest path in among the nodes. [30,31]. The main experiments in MANET are the with insignificant battery, so that attackers take a benefits of this deficiency, and challenges continue to keep them nodes conscious until all its energy lost and then node will enter into stablesnooze [18]. Many attacks in MANETs such as jellyfish attack, adaptation attack, misroute attack and routing table excess have been studied and shown [32, 33, 34].

With black hole attacks, a harmful node uses their routing protocol to supply the smallest path to the particular vacation spot node to the particular data in which it would like to discover. This intense node states its availability for the fresh tracks of its routing table. The attacker node will continually have the same procedure as follows [35, 36]. This paper is emphases on the study of malicious attacks in MANET for Reactive and Proactive protocols and comparesthe vulnerability of these.

2.3. Packet Encryption

The Rijndael Method is completely new Advanced Encryption Standard (AES) suggested with US National Institute of Standards and Technology (NIST) regarding incredibly sensitive. They have been employing some other encryption algorithms, such as DES (Data Encryption Standard), Multiple DES and also

Skipjack for encrypting crucial authorities' by using data to defend against any potential provocations for these kinds of algorithms from discovering innovative cyber-terrorist.

The true secret terms being pleased because of the presented algorithms being royalty-free, publicly-disclosed. These algorithms depending on symmetric crucial cryptography cipher and help dimensions to associate with 128-bits with crucial dimensions associated with 128-bits, 192-bits and 256-bits.Caused by this request, 15 candidate algorithms from the cryptographic joined up with the initial circular.

Inside November 2001, the National Institute of Standards and Technology (NIST) (NIST) regarding United States chose the Rijndael algorithm since the ideal AES [2] to switch the Data Encryption Standard (DES) algorithm [37].There are three kinds of choice for the cipher key of the AES: 128, 192 and 256bit, called AES128, AES192, and AES256, respectively [38]. AES has 10 rounds for 128bit keys, 12 rounds for 192bit keys, and 14 rounds for 256bit keys. The structure and also durability of crucial plans from the AES protocol tend to be enough to defend labeled details approximately the security level. AES provides three levels of security: 128, 192, and 256 bits. AESis the truncated memory in which its requirements willcreatewell-matched restricted space environments, for which the AES exhibits high performance. The AES algorithm is used in some applications such as smart cards, cellular phones and image video encryption. The efficiency of hardware implementations of the AES has been used by the designer as major criterion.

To determined [39] that AES is more rapidly and more effective than other encrypted Shield algorithms. If the communications of data areobservedwhen there is the insignificant variance in overall performance of unique symmetric key systems .The situation of data transfer isextremelyendorsed to use AES scheme forencrypting data which is kept at the other end and decrypted data at the manyintervals.

Theresearch [40] is agreed for dissimilar secret key algorithms such as DES, 3DES, AES, and Blowfish. They were combined, and their efficiency was associated by encrypting input files of varied contents and sizes. It was subjected to testing on two dissimilar hardware tools, for primarily research their efficiency. They had agreed out it on two dissimilar devices such as P-II 266 MHz and P-4 2.4 GHz. The results confirmed in which Blowfish got an amazing performance connected to various algorithms as well as proven in which AES got a greater efficiency than 3DES along with DES.That signifies that 3DES possesses nearly 1/3 throughput regarding DES, or even in other words it requires three times in comparison with DES to help course of action to related level of data [41].

There are several hardware implementations for AES that can be found in literature. These implementations were done for the original standard AES, such as the work presented in [42, 43, 44]. Before choosing Rijndael to be the AES in November of 2001, many related implementations were proposed to how much the structure of the proposed candidates for the AES competition is suitable for hardware implementation [45,46,47]. They provide a multiple architecture options for AES finalist candidates with an implementation analysis for each architecture based on both area and speed optimization. Also, the authors in [46] and [42] provided a detailed comparison of the FPGA hardware overall performance with the AES job hopefuls.

3. Overall Structure of Proposed Model

3.1. Selection of Secure and Authorized Node

To predict without loss of generality, a node takes the hash value of the node's current position and the current time when it receives a position request as its pseudo ID:

Pseudo ID = H (Node ID || present _position ID || present_time ID)

This operation guarantees that each pseudo ID is globally unique. Let us take a node refuses to report its position information, if a neighbor node requests it too frequently. We assume a node as a local buffer, which record its recently used pseudo IDs. In other words, a node is able to justify through the pseudo IDs which is used recently in processing. Inspite of using non-interactive zero knowledge technique is mainly used to detect the authorized nodes only. After linking with the MANET process, then the necessary procedure follows the above process. In this phase, there is need for authentication and hence the nodes with verifiable authentication are easy to determine nodes and they can have access to specific applications or services in a MANET. It can be performed by a suitable authentication protocol for MANET. The sender state begins by sending data to the destination immediately after the route set up has over. In source, every single packet is encrypted by symmetric session key SK_{SD} and is forwarded at each intermediate node to the next hop based to the route table. Next, receiving a packet, the next node maps the routine;many packets in its route table will establish its node to acts as a next hop. Due to the fact, the intermediate nodes does not know about the session key SK_{SD} so; it cannot decrypt the message, which maintains the privacy of the data. When the route is created, data will be forwarded with this route for a long time. If the IDs of the nodes do not change subsequently, opponents can still imagine that these nodes are maintaining an interconnection position and afterwards they share a similar relocating pattern by monitoring the communication traffic. In order to this movement visibility concern, IDs prerequisite to be improvednormally. In our scheme, the source node periodically updates its ID according to a certain fixed time interval *t*, which we called ID randomization interval, during the data transmission period. Once the ID has been modified, the source will start again a route demand message. The following nodes on path will therefore report their new IDs,thus, keeping track of possibility is minimized.

In Figure 2 in which **A, B** and **C** nodes are verified [48]. When node $\mathbf{X_1}$ enters the MANET, its authentication action is done by neighboring nodes **B** and **C**. For example, node $\mathbf{X_1}$arrives in MANET, Its authentication will be verified by their closest node is**B** and **C.** At that time node $\mathbf{X_1}$ is an authorized node in the network. In node $\mathbf{X_2}$, node$\mathbf{X_1}$ and node **B** which are the closest to node verify its identity. Both nodes$\mathbf{X_1}$ and $\mathbf{X_2}$ are verified as authorized nodes in the network, and then the routing and transmitting packets would be done through them. There are several suitable protocols for authentication in the MANET which can be used. Of course, it is necessary to use protocols with low complexity and non-interactive which would not produce excessive computational overhead in the network.

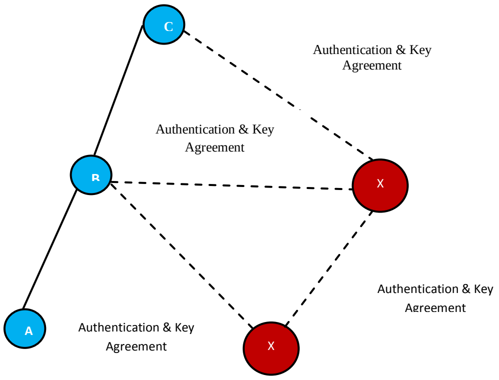

C
B
A
X
X
Authentication & Key Agreement
Authentication & Key Agreement
Authentication & Key Agreement
Authentication & Key Agreement

Figure 2: Entering new nodes X_1,and X_2 , to the MANET

For example, in Figure 2, the node $\mathbf{X_1}$ can prove its identity to the nodes B and C are guarantees that discrete logarithms of $y_1=\cdot_1^{x1}$ and $y_2=\cdot_2^{x2}$ are computed with $_1$ and$\cdot_2$ and bases are displaced in equation (1):$\boldsymbol{k_1.x_1+k_2.x_2=b\ (mod\ p)}$ ***………… (1) K1***and ***K2***are integers and *p* is the prime number [48]. In the above protocol, node $\mathbf{X_1}$first computes they_3 and y_4 ($y_3=._3x_3$, $y4=._4\ x_4$) then solves the equation (2) for integers $\boldsymbol{x_3}$and $\boldsymbol{x_4}$:$\boldsymbol{k_1.x_3+k_2.x_4=0(mod\ p)}$ ***…………………... (2)***

Then the following messages are exchanged:

$$B, \leftarrow CX1: y_5 = \propto_1^{x_3}, y_6 = \propto_2^{x_4} \text{ ………. (M1)}$$

$$B, \leftarrow CX1: y_7 = H(\propto_1, \propto_2, y_1, y_2, k_1, k_2, b, y_5, y_6) \text{ …… (M2)}$$

$$B, CX1: y_8 = x_3 - y_7 \cdot x_1 (\text{mod } p), y_9 = x_4 - y_7 \cdot x_2 (\text{mod } p)$$

…. (M3)

Node X_1 sends y_5 and y_6 to the B and C nodes. The following node receives the M1 message, compute the $y_7$with a one-way hash function and send M2 message to the node $\mathbf{X_1}$. Node $\mathbf{X_1}$by examining M1 validity builds the M3 message and sends $y_8$and y_9 to the B and C nodes. Node $\mathbf{X_1}$ convinces nodes B and C that it knows the discrete logarithms of y_1 with the $\cdot_1$ and $\cdot_2$ bases and also knows that these logarithms build a linear equation. This can be done through verifying the resulted proof of y_7, y_8 and y_9. It is easily seen that nodes **B** and **C** will be always successful in making an accurate proof by reconstructing $y_{10}=._1{}^{y8}.y_1{}^{y7}$and $y_{10}=._2{}^{y9}.y_2{}^{y7}$ then it is examined to see whether $y_7$is an equivalent to y_{12} wheny_{12}=H$(._1,._2,y_1,y_2,k_1,k_2,b,y_{10},y_{11})$and if the equation(3) is accurate: $k_1.y_8+k_2.y_9=-yb(mod\ p)\ldots.(3)$Firstly, it is seen that nodes B and C are always successful in making a reliable proof because $y_{10} = y_5$and $y_{11} = y_6$.

$$y_{10} =\propto_1{}^{y_8} \cdot y_1{}^{y_7{}^{y8,y1}} =\propto_1{}^{x_3-y_7\cdot x_1} \cdot \propto_1{}^{x_1\cdot y_7} =\propto_1{}^{x_3} = y_{5,}$$

$$y_{11} =\propto_2{}^{y_9} \cdot y_2{}^{y_7{}^{y9,y2}} =\propto_2{}^{x_4-y_7\cdot x_2} \cdot \propto_2{}^{x_2\cdot y_7} =\propto_2{}^{x_4} = y_{6,}$$

So

$$y_{12} = H(\propto_{1,} \propto_2, y_1, y_{2,} k_1, k_2, b, y_{10}, y_{11}) = H(\propto_{1,} \propto_2, y_1, y_2, k_{1,} k_{2,} b, y_5, y_{6)=} y_7$$

.In this way, nodes B and C compute y and compare it with y in M2 message.

Secondly, if the E attacker, which does not know x_1 and x_2, will be able to compute these proofs. Because reversing the y_7 one-way Hash function is difficult, we suppose that the $y_{10}$and y_{11}values before computing $y_7$in M2 message is constant and also it seems to be necessary when the y_{10} and y_{11} values are constant, nodes B and C would be prepared for other possible messages. But this notion means that E also can compute different presentations of the y_{10} and y_{11}based on *.1*, *y1* and *.2*, *y2*which indicate the knowledge of x_1 and x_2, discrete logarithms of y_1, y_2 based on *.1*, *.2* But this would contradict the hypothesis of E does not know $x_1$and x_2 .Thirdly, nodes B and C, for verification, will replace the responses y_8 and y_9 in the equation (3):

$$k_1 y_8 + k_2 y_9{}^{y_8 y_9} = k_{1.}(x_3 - y_7 \cdot x_1) + k_2 \cdot (x_1 - y_7 \cdot x_2)$$
$$= k_{1.} x_3 - k_1 \cdot y_7 \cdot x_1 + k_2 \cdot x_4 - k_2 \cdot y_7 \cdot x_2$$
$$= k_{1.} x_3 - k_2 \cdot x_4 - y_7 \cdot (k_1.x_1 + k_2.x_2)$$

From equation (1) and equation (2)= -$y_7.b$(mod p).And the identity of the node X_1 is known reliable. From successful authentication of node X_1 we conclude that the considered node is authorized to the specific applications in the MANET.

3.2. AES Enhancementusing an Iterative Layout

Figure 3 shows the block diagram of the different units of the variable AES based operations.

- The Input and Output interfaces take care of reading input data and writing encrypted output and are responsible for feeding the key logic. They are controlled by the data ready, cipher text-ready and control signals. When the bus puts a data to be read or write this signal is selected and the data are taken.
- Library Functions: the different AES functions in this library, such as Sub-Bytes, ShiftRows, ShiftRows, MixColumns, andAddRound Key are defined.
- S-box ROM: is the direct implementation of the substitution boxes using look-up tables, because all of the variable cases of the substitution bytes can be recomputed and can be stored in a look-up table.
- Key Expander is used to compute a set of round keys based on a ciphered key.
- Controller is used to generate control signals for all other units. Among other actions, the controller determines when to reset the cipher hardware, to accept input data and to register output results. Since the execution of Mix Column function is conditional (Figure 3), the controller decides whether the result obtained byMixColumn is to be used or ignored.
- AES Round is used to encrypt or decrypt input blocks of data.

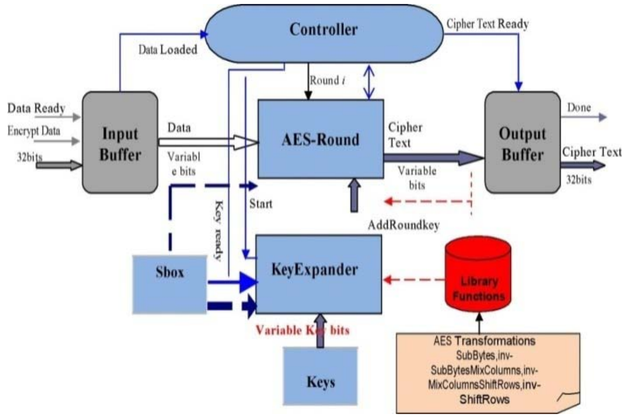


Figure 3.Proposal Structure of the ModifiedAES

In this approach the ECB/CBC mode of operations is employed for data confidentiality and authentication.

3.3. Modified Architecture

The encryption and decryption data path of the iterative variable AES core is based on the single round implementation of the AES algorithm. The same data path is the 14 rounds in the variable AES algorithm. Each round is performed in a single clock cycle except the first round that only do the key addition phase. The other 14 rounds perform the four different steps of the variable AES algorithm namely Sub Bytes, Shift Rows, Mix Columns, and AddRoundKey. Therefore, it takes total of 15 cycles to encrypt or decrypt a 256 bit block of data. Shows that the figure 4, five logic blocks compose the overall variable AES Round.

- The component implementing the function AddRoundKey is simply a net of XOR gates that adds in GF (2^8) the round key to the current state.
- The component implementing the function Sub Bytes uses 32 S-boxes stored in a Read Only Memory. The state obtained is row shifted.
- The Mix Columns function is implemented using a chain of XORs which results in the minimum delay implementation for this unit.
- The AES 256 encryption and decryption data path is optimized to have a minimum delay for each round.

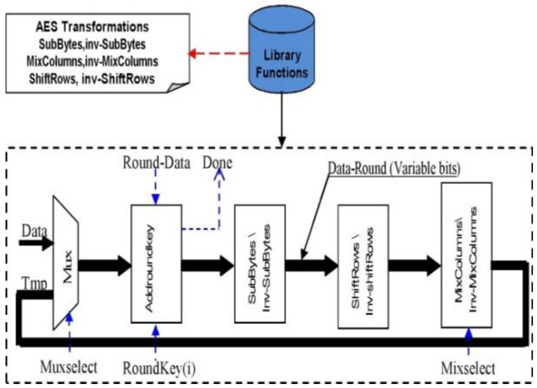


Figure 4. AES Round Operation

Overall, the total computational interruptions while using this AES 256 are minimized. The decryption process follows the same order as the encryption, except for another round of mixed columns on the generated round key.

3.4. Key Interchange and Communication

3.4.1. Key Generation and Distribution

The source node generates RREQ which is used to find the destination path by using broadcasting is shown in Figure 5. The packet from the source node is re-broadcasted in the neighboring node until it reaches the destination. A RREQ packet contains Source ID, Destination ID, Path, TTL and other information. Whenever the destination receives the RREQ packets it replies as RREP to the source. By this way it discovers a path by the source. Based upon the environment, different category of packets is generated according to the availability of route. Then the key is shared between source and destination. If it encounters the unavailability of packet then the source will generate and broadcast KRREQ which is supported to construct the route and key. Thus the destination will generate keys and send it to the source as many times as it receive the RKREQ/KREQ packet. The path and key information is updated in the route table periodically is shown in Table 1:

Next the source will combine all paths and keys to generate a secret key:

$$K_{SD}\int(P_1,P_2,P_{3,\ldots\ldots\ldots\ldots\ldots}P_N;K_{1,}K_2,K_{3,\ldots\ldots}K_N)$$

$$E_{ID}=E_{KSD}(\text{SourceID})$$

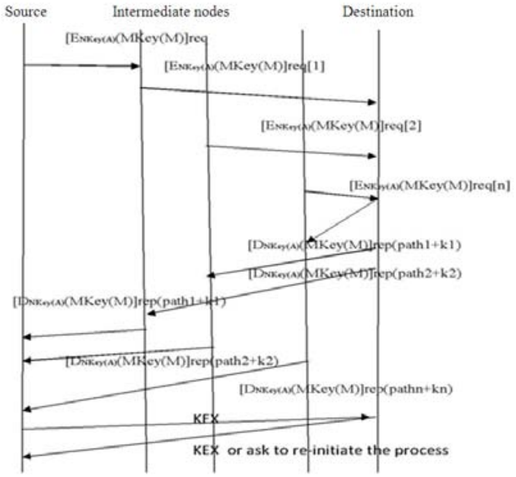

Source
Intermediate nodes
Destination
[ENKey(A)(MKey(M)]req
[ENKey(A)(MKey(M)]req[1]
[ENKey(A)(MKey(M)]req[2]
[ENKey(A)(MKey(M)]req[n]
[DNKey(A)(MKey(M)]rep(path1+k1)
[DNKey(A)(MKey(M)]rep(path2+k2)
[DNKey(A)(MKey(M)]rep(path1+k1)
[DNKey(A)(MKey(M)]rep(path2+k2)
[DNKey(A)(MKey(M)]rep(pathn+kn)
KEX
KEX or ask to re-initiate the process

Figure 5: Key generation and key exchange procedure

Source		Destination	
Path	**Key**	**Path**	**Kay**
P_1	K_1	P_1	K_1
P_2	K_2	P_2	K_2
P_3	K_3	P_3	K_3
…..	….	….	….
P_N	K_N	P_N	K_N

Table1. Routing table

$P_i \rightarrow$ = is the path from source to destination found in ith RREP packet

$K_i \rightarrow$ = is the key provided by the destination with ith RREP packet

$\int \rightarrow$ = Cryptographic key generation function

$E_{ID} \rightarrow$ = Encryption of Source_ID using K_{SD}

Destination will perform following operations

$$\int(p_1,p_2,p_3,\ldots\ldots p_n;k_1,k_{2,}k_{3,\ldots\ldots}k_n)$$

D_{ID} = D_{KSD}i(destination ID)

Pi→ = is the path from source to destination found in ith RREP packet

Ki→ = is the key provided by the destination with ith RREP packet

∫ - > = Cryptographic key generation function

D_{ID}- > = Decryption of Source_ID using K_{SD}

Once the key is shared, it is used for long period of time agreed by both party.

3.4.2. Encryption and Decryption for Key Exchange System

Key Exchange for the encryption and decryption algorithm is provided to secure the key.

3.4.2.1. Encryption Algorithm

Each node has its own symmetric key called neighborhood key which is encrypted. Source Node A creates a Message Specific Key[MKey(M)]. Message is encrypted with Message Specific Key [$E_{MKey(M)}$(M)]. Further the Message Specific Key is encrypted with A's neighborhood key [$E_{NKey(A)}$(MKey(M)].Then the ID is appended with that encrypted messageNode ID(destination).[([$E_{NKey(A)}$(MKey(M) $E_{MKey(M)}$(M)) Node ID(B)].

The following diagram shows how the message is encrypted and decrypted:

Encrypted Message $E_{NKey(A)}E_{MKey(M)}$(M) B at node B (MKey(M))

If B is the $D_{NKey(A)(}E_{NKey(A)}E_{MKey(M)}$(M) intended receipt (MKey(M)))

Decrypt with A's neighborhood Key

Decrypt messageMKey(M)DNKey(M) with the obtaind($E_{Mkey(M)}$(M))

If the node is not intended node it will switch over to another node:

If b is not $E_{NKey\ (A)}$ $E_{NKey\ (M)}$ (M) Cthe intended (MKey (M) recipient, ID

Decrypt the message

$D_{NKey\ (A)}$ EMKey $_{(M)}$ (M) Ckey with A's ($E_{NKey\ (A)}$ neighborhood key

(MKey (M)))

Re-encrypt the $D_{NKEY\ (B)}E_{MKey\ (M)}$(M) C message with B's (MKey (M) neighborhood key.

3.4.4.Neighborhood Key Exchange Procedure

The exchange of key with only neighborhood nodes is to reduce the overhead occurence while sending and receiving data to minimize crypto functions. This neighbourhood scheme is easy and is carried out at handshake process between any pair of neighbors. Handshaking is the process of exchanging key between nodes and neighbhour. After that each node shared the secret key and HELLO messages are sent frequently to the node in the group.To send and receive the data between source and destination, RREQ and RREP messages are used.

3.4.5. Decryption Algorithm

At receiver side ID is used to verify the destination ie whether it matches or not,if it matches, then decryption will start and provide the plaintext messages.otherwise re-encryption takes place with neighborhood key and transmits to its authenticated neighbor nodes. Decyrption is the reverse process of encryption in which is decrypt the message key as well as the node keys.

The following specifies the decryption:

[($D_{NKey(A)}$ (MKey(M) $D_{MKey\ (M)}$(M)) Node ID (source)].

4.Experimental Layout and Result Evaluation

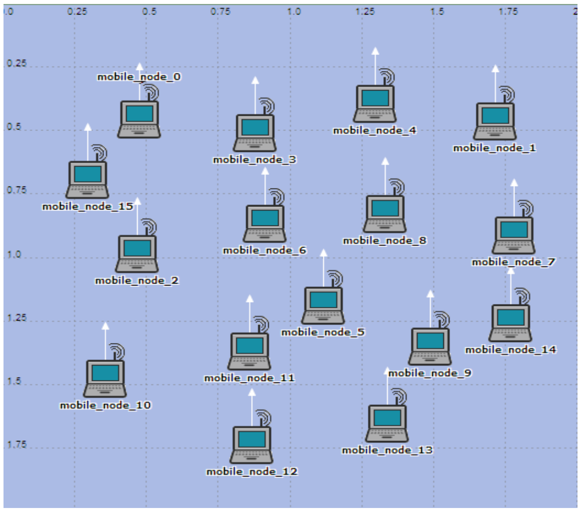
4.1. Simulation Tool

To simulating the OPNET 14.5 modeler is used with the support of a software. Normally OPNET is a program and structured software package that is used for managing and investigation[49]. An OPNET model provides communication devices, numerous protocols, architectural mastery of several networks and technological innovation and it provides simulation of their tasks in an exclusive settings. In a range of exploration to development areas, OPNET is commonly yields the particular alternative which in turn helps in exploration connected with research in addition to improvement of wi-fi technologies such as Wi-MAX, Wi-Fi, UMTS, evaluation in addition to acquiring with MANET methods, strengthening when prinicple of network technology know-how, supplying electric power administration solutions in wi-fi sensor networks.

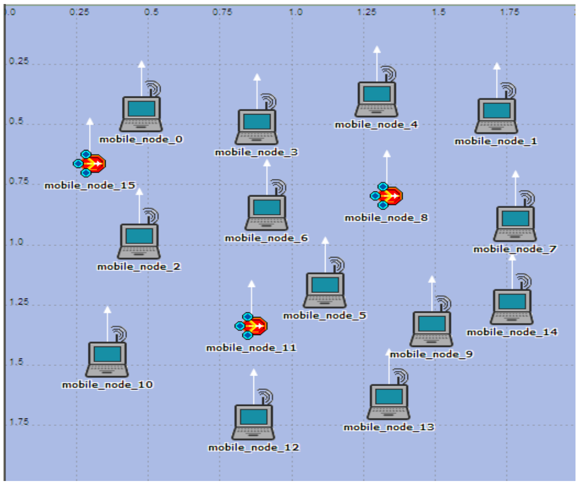
4.2. SimulationEnvironment

By this qualifying measure, we applied OPNET for modeling of network nodes, choosing its studies and then working its equivalent simulator to get the result of their effect for analysis.The simulation environment includes 20 nodes which act as client and one node as server. All nodes run on a TCP/IP or UPD/IP network. An 11 Mbps data rate is maintained for nodes, and their transmission power of 0.005 watts and reception power threshold set at -95dBm is maintained. Nodes are mobile at random trajectories. FTP traffic was generated randomly. Experiments simulated geographic routing protocol with all nodes cooperating and only15% of them are being malicious. Figure 6 and Figure 7 shows simulation setup test bed with one server node and 20 client nodes without attack node and with attack node. Thereveals simulation values from the first six minutes simulation.

To contemplate the simulation area of dimension is taken as 1000 x 1000 meters. Packet Inter-Arrival Time (sec) is obtained rapid (1) and packet size (bits) is rapid (1024). Random way point mobility is the way to choose with the frequent speed of 10 meter/seconds and minimal pause time of information of 100 seconds.



After achieved data to the destination, the equivalent pause time is considered. Our aim was to establish the protocol for the minor amount of vulnerability in situation of malicious attacks. GRP routing protocols is used for deciding whether the protocol is reactive and proactive. Within the scenarios regarding GRP, detrimental node buffer measurement would be the minimal levels which can be to enhance the particular bundle decline. Moreover, the simulation particulars are shown in Table 2.



From the Figure.6, the outline used in our Simulated Setting with 20 Nodes. From the Figure.7, theoutline used in our Simulated Setting with 20Nodes with Attacks.

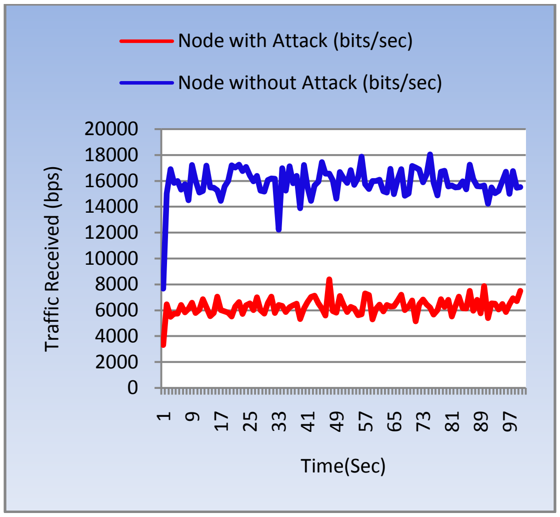
Simulation Parameters	
Tested Protocol	GRP
Time	1000 seconds
Area (m x m)	1000 x 1000
Number of Nodes	20
Travel Type	TCP/IP or UPD/IP
Performance Factor	Traffic Sent and Received , Retransmission Attempts and Throughput
Pause Time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival	exponential(1)
Time(s)	exponential(1024)
Packet Range (bits)	0.005
Transmit Power(W)	11 Mbps
Date Rate (Mbps)	Random waypoint
Mobility Model	
Power Threshold	-95dBm

Table 2. Simulation parameters

Figure 8 to Figure 10 disclose network performance with regard to traffic received, sent, retransmission attempts and throughput respectively. The graphs show that network performance is degraded, and throughput is drastically reduced before attacking malicious nodes. We evaluate the following three metrics: traffic sent and receive throughput measurement and packet retransmission.

4.3. Traffic Sent and Received Packets

From figure 8, it describes that the routing traffic is transmitted from various sources to destinations decreases by 39.63% owing to the presence of malicious nodes. The actual network insert graph associated with GRP together with in addition to avoid of reputation of a malicious node continues to be proved in network. In the event of 20 nodes this network insert associated with GRP is usually three times greater in the case of avoid of episode which in turn implies that it must be truly redirecting in the bundle on the entire correct location. Butin attack, it cannot send its packet i.e. packet disposal leads to a decrease of network load. In situation of 30 nodes there is a slight distinction in between GRP with and without attack. This is owing to the high number. of nodes which leads to more increase in routing traffic.



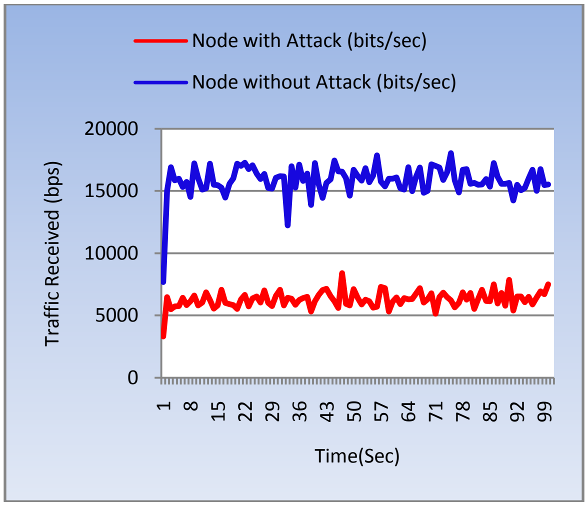


Figure 8. Traffic sent and received packets

4.4. Performance of Packet Retransmission

In network, routing involves malicious attacks and without having attacks is dependent around the method redirecting technique and variety of nodes included. Interval in circumstance of 20 nodes with regard to GRP is actually high in circumstance if you find absolutely no attack around the network nodes. Thisindeed is simple because the malicious attacksshouldnot have about RREQ's in addition to RREP's because the malicious node at the moment transmits its RREQ's on the sender node prior to a destination node respond acquiring fewer intervals. From the figure 9, 30 nodes, the delay is 5 percent much more as compared to the 20 nodes. The overall result ondelay over GRP is similar as it was noticed in 20 nodes. The maximum numbers of nodes also increases the variation of delay in GRP in scenario of malicious attack with evaluation to a simple GRP scenario.

The results indicate the typical packet end-to-end delay in a malicious node only. This is reliable if the numbers of nodes are less. However, with the increase in number of nodes.The delay of GRP is also increased. For 30 nodes, GRP show excessive delay in evaluation with a simple GRP situation. In the delay, the efficiency of GRP helps with the increase in number of nodes for the reason that of its table driven dynamics. The idea saves current direction-finding facts through each and every node to be able to some other node within the multilevel.

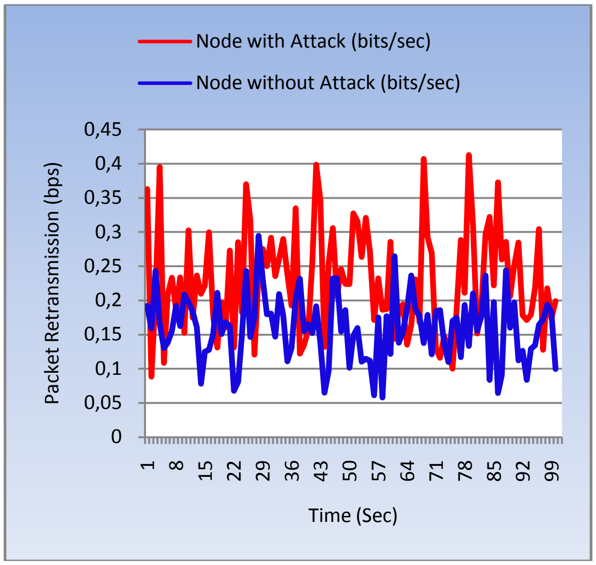


Figure 9.Packet retransmission attempts

4.5. Performance of Throughput Measurement

Form the figure 10, the 20 nodes is really crystal clear in which the throughput pertaining to GRP will be substantial in the network without attack. That is mainly with the lesser amount of redirecting forwarding along with redirecting targeted visitors.

The actual malicious node discards the information as an alternative in comparison with forwarding that on the destination, thus impacton throughput. Similarly using for 30 nodes, the throughput is high for the sophisticated number of nodes but the development of throughput with attack and without attack endures to be the exact same as in 20 numbers of nodes.

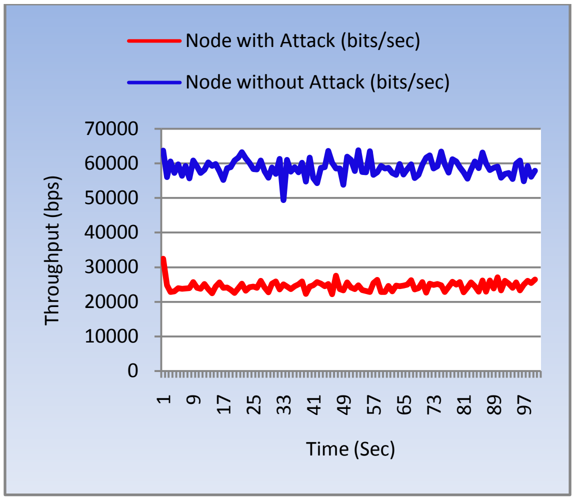


Figure 10. Throughput Measurement

It is observed for the simulation results that the routing traffic sent from various sources falls by 39.9% owing to the presence of the malicious nodes. Since routes could not be created for random traffic from various sources to destinations, the throughput of the network falls down by 41.8% when the network contains 15% malicious nodes.

4.6. Performance Analysis of Modified variable AES Algorithm

4.6.1. Security

Hence using of variable key size and block size for the security has to be enhanced. And the linear cryptanalysis and differential cryptanalysis require more time then Rijndael to break our proposed cipher.

4.6.2. Technique Comparison

To encrypt a packet, the amount of time is proportional to the number of bytes in the packet. If the packet size is variable long then our proposed algorithm has to execute once. To Rijndael algorithm has to run twice to encrypt the whole data. In our proposed algorithm shows more efficient. The difference of the efficiency is negligible. But our proposed cipher is much efficient than Rijndael algorithm. The simulated result is given below through the figure 11 and 12.

4.7. Experimental Results

The Encryption Algorithms have been tested with various sizes oftext files and it shows the respective results of different file sizes. Comparison of throughput has been explained in the following and also the execution time of various encryption algorithms on various sizes of text files.

4.7.1. ThroughputAnalysis

4.7.1.1. AverageThroughput:

The ratio of the number of messages received by the destination to the number of the messages sent out by the source. $D_i$and $S_i$represent destination $i$and source i, respectively.

$$avgPDR = \frac{1}{S}\sum_{i=1}^{S}\frac{|M_{received\_D_i}|}{|M_{sent\_S_i}|}$$

4.7.1.2. EncryptionProcess

The Produced results for this comparison points are shown Figure.11 and Table 3 at encryption stage. The Rijndael algorithm has low performance in throughput when compare with Variable AES algorithm. It requires always more time than Rijndael algorithm because of its key size values.

Input size (in bytes)	**Rijndael**	**Variable AES**
138 Bytes	16	13
171 Bytes	22	14
181 Bytes	24	15
190 Bytes	25	17
202 Bytes	27	19
216 Bytes	30	21
229 Bytes	33	21
Average Time	**25.28Sec**	**16.14Sec**
Throughput (Bytes/sec)	**52.494 Bytes/Sec**	**82.219 Bytes/Sec**

Table 3: Executiontimes of encryption with different packet Size

The following figure.11 shows that results obtained from running the program using different data loads. The result shows the impact of changing data loads on each algorithm. The encryptionand decryption modes are used.

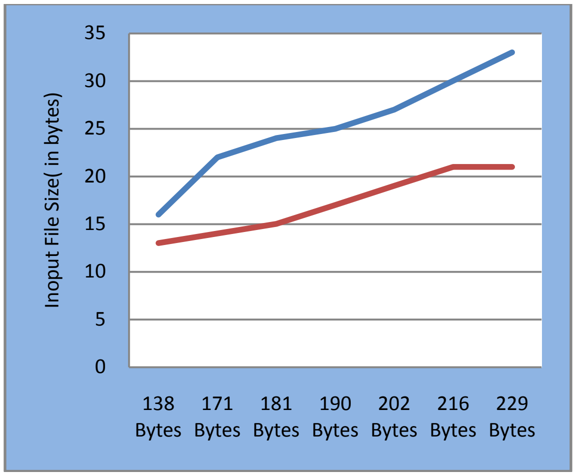


Figure 11: Throughput of Rijndael vs. variable AES.

4.7.1.3. Decryption Stage

The Produced results for this comparison points are shown Figure.11 and Table 4 at decryption stage. In decryption, the Variable AES algorithm is better than Rijndael algorithm in throughput and Rijndael algorithm still requires more time than variable AES algorithm.

Input size (in bytes)	Rijndael	Variable AES
240 Bytes	18	14
266 Bytes	23	16
282 Bytes	27	17
295 Bytes	31	20
305 Bytes	35	23
324 Bytes	38	25
338 Bytes	41	28
Average Time	**30.429 Sec.**	20.429 Sec
Throughput (Bytes/sec)	**67.367 Byes/Sec**	**106.853 Bytes/Sec**

Table 4: Executiontimes of decryption with different packet Size.

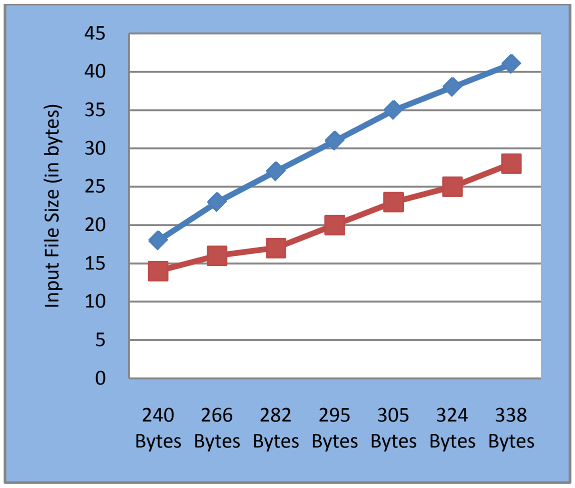


Figure 12: Throughput of Rijndaelvs. variable AES

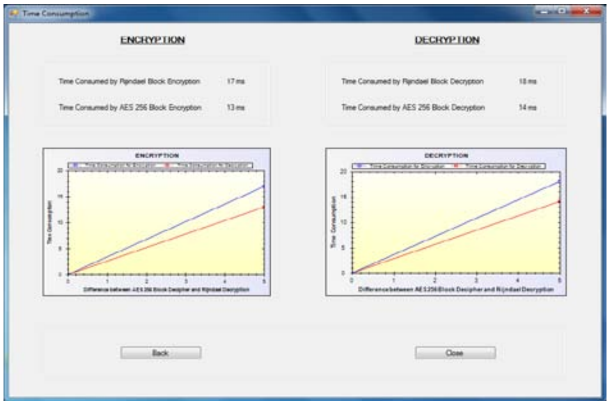
4.7.1.4. Time Consumption

Average Delay: Including the transmission and delay for all types of messages transmitted.

$$avgD = \frac{1}{s}\sum_{s=1}^{S}\left(\frac{1}{dM_s+rM_s}\left(\sum_{m=1}^{rM_s}\left(T_{Sign_{m\_s}} + T_{Trans_{m\_s}} + T_{verify_{m\_s}}\right) + \sum_{m=1}^{dM_s}\left(T_{enc_{m\_s}} + T_{trans_{m\_s}} + T_{dec_{m\_s}}(|queue|)\right)\right)\right)$$

Where, *avgD* is average transmission delay, *s*is the number of source nodes, and $rM_s$and dM_s is the number of routing messages and data packets incurred by source *s*, respectively.

Rijndael algorithm and Variable AES are compared with time consuming in calculating encrypted file and their results are shown in the following Figure.13. From this graph, it is analyzed that both Encryption and Decryption Response Time of Variable AES algorithm is less than Rijndael algorithm.


Time Consumption
ENCRYPTION
Time Consumption for Encryption
Time Consumption for Decryption
Time Consumption
20
15
10
5
0
0 1 2 3 4 5
Difference between AES 256 Block Decipher and Rijndael Decryption
DECRYPTION
Time Consumption for Encryption
Time Consumption for Decryption
Time Consumption
20
15
10
5
0
0 1 2 3 4 5
Difference between AES256 Block Decipher and Rijndael Decryption
Back
Close

ENCRYPTION

Time Consumed by Rijndael Block Encryption 17 ms

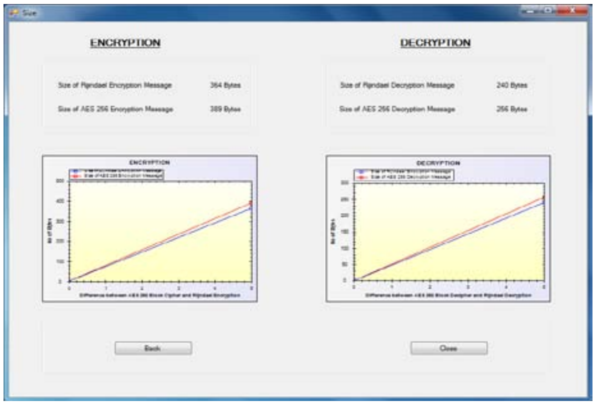
Time Consumed by AES 256 Block Encryption 13 ms

DECRYPTION

Time Consumed by Rijndael Block Decryption 18 ms

Time Consumed by AES 256 Block Decryption 14 ms

Figure 13 : Response time of Rijndael algorithm vs. variable AES.


Size
ENCRYPTION
Size of Rijndael Encryption Message
Size of AES 256 Encryption Message
No of Bytes
500
400
300
200
100
0
0 1 2 3 4 5
Difference between AES 256 Block Cipher and Rijndael Encryption
DECRYPTION
Size of Rijndael Decryption Message
Size of AES 256 Decryption Message
No of Bytes
300
250
200
150
100
50
0
0 1 2 3 4 5
Difference between AES 256 Block Decipher and Rijndael Decryption
Back
Close

ENCRYPTION

Size of Rijndael Encryption Message 364 Bytes

Size of AES 256 Encryption Message 389 Bytes

DECRYPTION

Size of Rijndael Decryption Message 240 Bytes

Size of AES 256 Decryption Message 256 Bytes

Figure 14.Packet Size of Rijndael algorithm vs. variable AES.

4.7.1.5. Packet Size

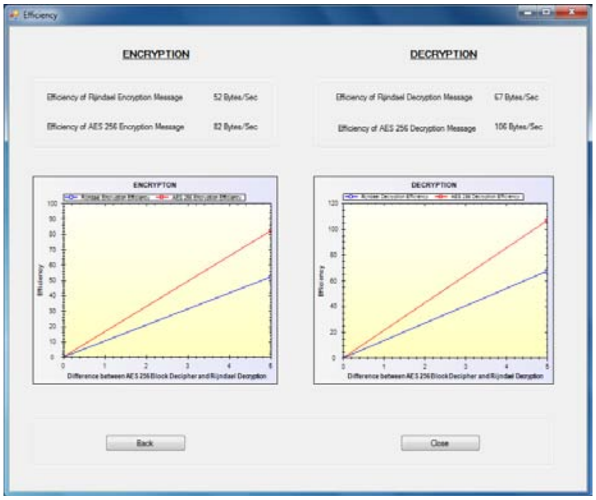
In Figure 14, we demonstrate that the overall recital of cryptographic algorithms in phrases of CPU process time. It demonstrations the CPU load. Variable AES is need further time to encrypt dense size files and also need much more time to encrypt huge file sizes.Because of this Variable AES is useful for encrypting big data by Rijndael. Much more over for big files, CFB and CBC normally takes virtually equivalent occasion however ECB will take a smaller amount occasion when compared with both of these. For compact data, time needed by ECB and CBC is identical. Figure 14.Shows the experimental results for CPU process time for the interval of decryption. From the results we found that the successes are almost same as in the encryption method. And Variable AES is improved when compared to Rijndael.

Rijndael algorithm and Variable AES arecompared to size after performing Encryption and decryption and their results are shown in the figure 14. From this graph, it is analyzed that both Encryption and Decryption Size of Variable AES algorithm is less than Rijndael algorithm.

4.7.1.6. Efficiency

Within figure15, indicates your performance involving cryptographic algorithms with regards to encryption time period and decryption time period. In this article, this encryption time period regarding with varying AES with Rijndael protocol result in difference file sizing. Rijndael will take much less proficiency regarding bytes to encrypt in addition to decryption will be Varying AES. In AES, CFB in addition to CBC will take almost equivalent time period however ECB will take much less time period than both of these.

Rijndael algorithm and variable AES algorithm are compared with efficiency in calculating encrypted file and their results are shown in the following figure 15.From this graph it is analyzed that both Encryption and Decryption efficiency of Variable AES is more than Rijndael algorithm.



Efficiency

ENCRYPTION

Efficiency of Rijndael Encryption Message 52 Bytes/Sec

Efficiency of AES 256 Encryption Message 82 Bytes/Sec

DECRYPTION

Efficiency of Rijndael Decryption Message 67 Bytes/Sec

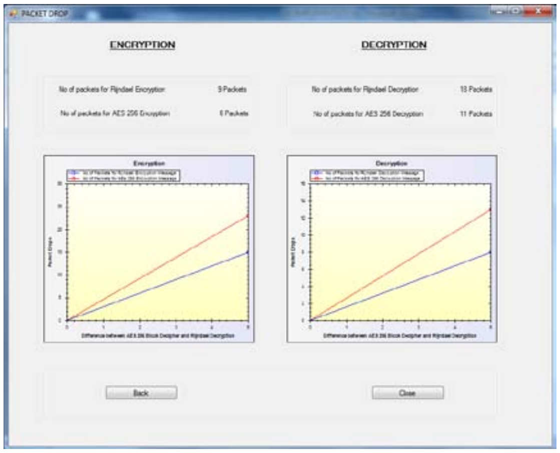
Efficiency of AES 256 Decryption Message 106 Bytes/Sec

ENCRYPTON
Efficiency
Difference between AES 256Block Decipher and Rijndael Decryption
DECRYPTION
Efficiency
Difference between AES 256Block Decipher and Rijndael Decryption
Back
Close

Figure 15.Efficiency of Rijndael algorithm vs. variable AES.

4.7.1.7. Packet Drops Comparison

Rijndael algorithm and Variable AES algorithm is compare with the packet drop in calculating encrypted file and their results are shown in the following Figure 16. From this graph it is analyzed that both Encryption and Decryption packet drop of Variable AES algorithm is less when compared to Rijndael algorithm.



PACKET DROP

ENCRYPTION

No of packets for Rijndael Encryption 9 Packets

No of packets for AES 256 Encryption 6 Packets

DECRYPTION

No of packets for Rijndael Decryption 13 Packets

No of packets for AES 256 Decryption 11 Packets

Figure 16. Packet drop of Rijndael algorithmvs. variable AES.

The result conclusion of this paper is achieved by overall throughput and it is improved by using the proposed method on Geographic Routing Protocol and also achieved the throughput as same as show in Figure 17.

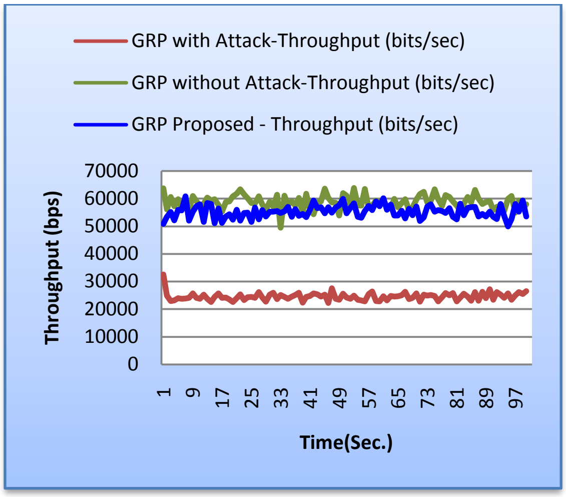


Figure 17.Overall throughput achievement by using proposed method.

5. Conclusion

There are many geographic routing protocols proposed for MANET. The proposed GRP is characterized by the ability toensurefor both the locationand identity privacy for the users. In-spite of identifying the authentication nodes which is used to provide the security and find the attackers in MANET. In this paper, the proposed schemeis non-interactive zero knowledge technique to exchange information for their authentication and found the attackers. Further, the simulation of the study is to obtain the performance degradation with GRP and throughput is reduced significantly owing to these malicious attacks. In this proposed algorithm, throughput is improved by using asymmetric encryption method for secure packet transmission.

6. References

[1] J. Blum, A. Eskandarian, and L. Homan, "Challenges of intervehicle ad hoc networks," IEEE Transactions on Intelligent Transportation Systems, vol. 5, no. 4, pp. 347 – 351, Dec. 2004.

[2] M. Mauve, J. Widmer and H. Hartenstein, A Survey on Position Based Routing in Mobile Ad-hoc Networks, IEEE Network Magazine, 15(6):30–39, November 2001.

[3] C. Perkins and E. Royer, "Ad-hoc on-demand Distance Vector Routing," Proc. 2nd IEEE Workshop. Mobile Comp. Sys. App., Feb. 1999, pp. 90–100.

[4] D. Johnson and D. Maltz, Mobile Computing, Chap. 5 — Dynamic Source Routing, Kluwer
Academic Publishers, 1996, pp. 153–81.

[5] Z. Haas and M. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," ACM/IEEE Trans. Net., vol. 9, no. 4, Aug. 2001, pp. 427–38.

[6] E. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad Hoc Wireless Networks," IEEE Pers. Communications, Apr. 1999, pp. 46–55.

[7] J. Broch et al., "A Performance Comparison of Multi-hop Wireless Ad Hoc Network Routing Protocols," Proc. 4th ACM/IEEE Int'l. Conf. Mobile Computing and Networking MOBICOM '98, Dallas, TX, USA, 1998, pp. 85–97.

[8] E. Kaplan, Understanding GPS, Artech House, 1996.

[9] S. Capkun, M. Hamdi, and J. Hubaux, "Gps-free Positioning in Mobile Ad Hoc Networks," Proc. Hawaii Int'l. Conf. System Sciences, Jan. 2001.

[10] J. Hightower and G. Borriello, "Location Systems for Ubiquitous Computing," Computer, vol. 34, no. 8, Aug. 2001, pp. 57–66.

[11] C. E. Perkins, "Ad Hoc Networking", Addison-Wesley, 2001, ISBN 0-201-30976-9

[12] E.M. Royer, C.-K Toh: "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks",
IEEE Personal Communications, April 1999.

[13] X. Lin, R. Lu, P. H. Ho, X. Shen, and Z. Cao, "ASRPAKE: An anonymous secure routing protocol with authenticated key exchange for wireless ad hoc networks," *Proc. IEEE ICC '07*, Glasgow, UK, 2007.

[14] B. Karp, and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," *Proc. Of mobile computing and networking (MobiCom '00)*, pp. 243-254, 2000.

[15] D. Boneh and M. Franklin. "Identity based encryption from the Weil pairing," *SIAM Journal of Computing*, Vol. 32, No, 3, pp. 586-615, 2003.

[16] M.N. Islam, M. Mia, M. Chowdhury, M.A.Matin, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology"Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008(SNPD '08). 6-8 Aug. 2008, PP.291 – 294, Phuket, Thailand.

[17] M. Mauve, J. Widmer, and H. Hartenstein, (2001) "A survey on position-based routing in mobile ad hoc networks", IEEE Network Magazine, Vol. 15, Issue No.6, pp. 30-39.

[18] X. Hong, K. Xu, and M. Gerla, (2002) "Scalable Routing Protocols for Mobile Ad Hoc Networks", IEEE Network Magazine, vol. 16, no. 4, pp. 11-21.

[19] C. Lochert, H. Hartenstein, and J. Tian, (2003) "A Routing strategy for vehicular ad hoc networks in city environments", Proceedings of IEEE Intelligent Vehicles Symposium, Columbus, USA, pp. 156-161.

[20] Y. Ko, and N. Vaidya, (2002) "Location Aided Routing in Mobile Ad Hoc Networks", ACM journal of Wireless Networks, vol. 6, no. 4, pp. 307-321.

[21] Li. F., Wang.Y. (2007): Routing in Vehicular Ad Hoc Networks: A Survey. IEEE Vehicular Magazine.

[22] Olariu S., Weigle M. C. (2009): Vehicular Networks: From Theory to Practice. CRC Press, a Chapman & Hall Book.

[23] Karp B., Kung H.T. (2002): GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. MobiCom.

[24] Raw R.S., Lobiyal D.K., (2010): VANET: Position-Based Routing in c Urban Environment – A Technical Review. TRANSTEC 2010, New Delhi.

[25] P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

[26] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.

[27] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007

[28] S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks".

[29]M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks," Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[30] N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad-Hoc Network".

[31] V.Mahajan, M.Natue and A.Sethi, "Analysis of Wormhole Intrusion attacks in MANETs," IEEE Military Communications Conference, pp. 1-7, Nov, 2008.

[18] F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, pp. 22-26, Apr, 2002.

[32] H.L.Nguyen, U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks," International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr, 2006.

[33] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[34] H.Deng, W.Li and D.P.Agrawal, "Routing Security in Wireless Ad-Hoc Networks," University of Cincinnati, IEEE Communication Magazine, Oct, 2002.

[35] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.

[36] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006.

[37] National Institute of Standards and Technology (NIST). Data Encryption Standard (DES).Federal Information Processing Standards Publications (FIPS PUBS) 1999.

[38] National Institute of Standards and Technology (NIST). Advanced Encryption Standard (AES). Federal Information Processing Standards Publications (FIPS PUBS), 2001.

[39] S. Hirani, Energy Consumption of Encryption Schemes in Wireless Devices Thesis, University of Pittsburgh, Apr. 9, 2003, Retrieved Oct. 1, 2008. (http://portal.acm.org/citation.cfm?id=383768)

[40] A.Nadeem, A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, pp. 84-89, 2006.

[41]Results of Comparing Tens of Encryption Algorithms Using Different Settings- Crypto++ Benchmark, Retrieved Oct. 1, 2008. (http://www.eskimo.com/ weidai/benchmarks.html).

[42]M.Bean et al. "Hardware Performance Simulations of Round 2 Advanced Encryption Standard Algorithms (Nov2001).

[43]J.Daemen and V.Rijmen "The Rijndael Block Cipher: AES Proposal ", Pro 1st AES Candidate conference 1998.

[44]H.Kuo and I.Verbauwhede "Architecture Optimization for a 1.82 Bits/Sec VLSI Implementation of the AES Rijndael Algorithm" Cryptographic Hardware and Embedded Systems (CHES2001), Lecturers Notes in Computer Science 2162 , Springer –Verlag , Heidelberg Germany 2001, pp.53-67.

[45]J.Elbert , W.YipB.Chetwynd ,C.Paar ,"An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists, IEEE Transactions on VLSI Systems , Vol. 9, No.4, pp.545-557, August 2001.

[46]K.Gaj and P.Chodowiec "Comparison of the Hardware Performance of the AES Candidates using Reconfigurable Hardware " Proc. 3rd Advanced Encryption Standard Conference , New york, April 2000, pp. 40-54.

[47]Dandali A., Prasanna V.K. Rolim J.D, " A Comparative study of Performance of AES Final Candidates using FPGAs Cryptographic

Hardware and Embedded Systems workshop (CHES2000) Worcester Massachusets 2000.

[48]Komninos, N., D. Vergados and C. Douligeris, 2007. Detecting Unauthorized and Compromised Nodes in Mobile Ad Hoc Networks. Elsevier Ad hoc networks, 5(3): 289-298.

[49] Opnet Technologies, Inc. "Opnet Simulator," Internet: www.opnet.com, date last Viewed: 2010-05-05.