IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Performance Modelling of Secure Routing Protocol in Communication Network

Mukesh Dixit[1*], Sarvottam Dixit[2], Ajay Kumar Sachan[3]

[1]Dept. of Computer Science & Engineering, Mewar University, Chittorgarh, Rajasthan, India
[2]Dept. of Computer Science & Engineering, Mewar University, Chittorgarh, Rajasthan, India
[3]Dept. of Computer Science & Engineering, LNCT College, RGPV University, Bhopal, India

[*]*Corresponding Authors: mukesh_dixit110@yahoo.co.in*

Available online at: www.ijcseonline.org

Accepted: 19/Nov/2018, Published: 30/Nov/2018

***Abstract* -** A mobile ad hoc network is not a wired network it's a wireless network that uses multiple hops, peer-to-peer routing in its place of motionless network infrastructure to present network connectivity which is used by consumer for communication. Here, we are discussing and designing newest MANET routing protocols along with is comparisons from previous routing protocol as well as discussed improve version of MANET routing protocols e. g. DYMO is the extended version of AODV and Encrypted DYMO(E-DYMO) is improved version of proposed DYMO; earlier than some routing protocols are synchronized by simulations. Network Simulator (Version 2) present a extremely modular platform intended for wired as well as wireless simulations following different - different network essentials, traffic, protocols, along with routing types. In this work, we get the simulation results in terms of various parameters like throughput, PDR, and E2E delay in terms of security of routing protocol. We also describe comparisons between Enhance DYMO, E-DYMO and proposed DYMO in terms of given parameter as well as shows that the enhance the security of various parameters along with proposed DYMO.

Keywords - MANET, AODV, Proposed DYMO, E-DYMO, Security.

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are composed of a huge variety of devices or gadgets that act as dynamic nodes with limited processing abilities that could exchange or share the information or info or data among each other. In this dissertation focused on coding which is related to the communication network and also easy to implement, simple to understand and also that would have used for security of the data generally known as data confidentially. Ad hoc networks [1] basically make to use of self-representing nodes so that network used to self-guide with no infrastructure. Along these lines, specially allotted systems that have network with a dynamic topology with the end goal this nodes can undoubtedly join or leave the system whenever. They have numerous conceivable applications, particularly, in military and protect regions, for example, associating troopers on the war zone or setting up another system set up of a system which crumbled after a fiasco like suddenly an Earthquake.

Especially ad-hoc networks are appropriate for zones where it isn't conceivable towards setting up a settled framework. While the computer or nodes broadcast with one to other without using an infrastructure then they provide the ad-hoc network by transfer packets over themselves. For ad-hoc network some of the protocols used to assist its

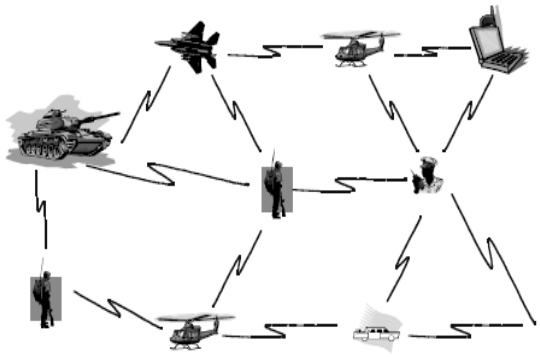

Figure 1: Mobile Ad-hoc Network structure

network, computer or nodes can use of some routing protocols for example like DSDV (Destination-Sequenced Distance-Vector), DSR (Dynamic Source Routing), AODV (Ad-hoc On-Demand Distance Vector). Each node similarly going toward in switches after that we find a path & forward all packets to the right computer or nodes in the ad-hoc network. This paper represent various sections; Section I contains the introduction of mobile ad hoc network and its various routing protocols along with its advantages, section

II describe the literature survey, section III represent Encryption Algorithm Based on Permutation Scheme (PPE) on Proposed DYMO, section IV shows simulation results and its parameter and section V concludes our research work.

1.2. Advantages of MANET over Wired Network [2, 3]

Many of the extensive feature & advantages of Mobile Ad-Hoc network has been in comparison to the wired network are follow:

1). Remote Areas

To setting up an infrastructure in sparsely populated areas may possibly too expensive so proper network will be given more benefitted for set up an infrastructure. So basically it Depend on which type of the communication pattern are we used. the mobile ad- hoc networks and satellite infrastructures be capable of this type of network.

2). Effectiveness

Generally network services provide by a existing infrastructures may be too costly for many of certain application. Have look an example we see merely connection oriented cellular or mobile network are exists, nevertheless mobile application send only small piece of information each minute. So ad-hoc network is a best & cheaper ad hoc packet-oriented network may be a good solution. Their Registration process could take too much time. For communication costs may be too much high amid active networks. ad hoc networks Application-tailored give a good solution.

3). Instant infrastructure

While an unplanned meeting will organize or instant or spontaneous inter personal communications will be happen then instant infrastructure facility available in MANET ad-hoc network .generally we cannot depend on any of infrastructure. Before setup an Infrastructures proper planning & administration required. Because setup a new infrastructures would take more time hence MANET-ad- hoc Network connectivity is instant solution.

4). Disaster Relief

When suddenly earthquake or disaster occurs most of the Infrastructures normally break down in disaster area. That time most of the wired line, power line will hurricane cut phone and flood totally demolish base stations, fire burns computer servers. So during the disaster Emergency teams might be depending on infrastructure they can set up themselves. There was no planning can be made & the setting up an infrastructure have to be particularly quick and reliable. The similar type of infrastructure need to apply in many of the activities in military cant. So that was the main reason to introducing mobile ad hoc networking researching in mobile communication.

1.3. MANET Features [2]

MANET AD-hoc network provide better quality & it has the some silent features which give network infrastructure more reliable & secure network .these feature are following:

1). Autonomous or Self Dependent Terminal

One of the best features in MANET ad-hoc network is autonomous where each of mobile terminals or node has an autonomous node, so it has a unique function as both a router & a host. In other term in addition to the basic processing capability as a host and the mobile terminal or nodes be capable of to perform switching functions as a router. Accordingly the endpoints & switches are impossible to differentiate in MANET.

2). Distributed Operation

Because there is no background set of connections for the central organize of the network operation, to proper management of network & controlling of the network is totally distributed amongst the computer nodes & terminals. The existing nodes which are involved in a MANET ad-hoc network should be collaborate in between themselves and every computer node or terminal act as a pass on when it required. for implementation functions for example network security and data routing.

3). Multi Hop Routing

Essentially ad hoc routing algorithms used two type of routing algorithm. First is a single-hop & other one is multi hop basically it depend on different type of link layer their attributes & routing protocols used. The first Single-hop MANET is simple in comparison to multi hop. Here we talk about structure pattern and implementation strategy & amid the charge of slighter applicability & functionality. While delivering a data packet from one end source to other end destination away of the direct wireless transmission network range then the packets have to be forward through either one or many intermediate nodes.

4). Dynamic Network Topology

As we know that here our nodes are mobile, so using mobile the network topology may be change quickly & their unpredictably. The connectivity between the node and terminals may change with point in time. MANET ad-hoc network should adjust the traffic & broadcast condition along with the mobility pattern of the mobile net of nodes. The mobile nodes or terminal dynamically set up routing in the network amongst them where ever they move from one place to other place.

5). Fluctuating Link Capacity

Since the wireless connection is a high bit-error rates so may be more reflective in a MANET. So the path or route from one end source to other end destination can be shared by several of sessions. It has fewer bandwidths in compare to wired network.

The communication channel over which is the terminals communicate is subject to fading, and interference, noise.

6). Light-weight Terminal
In a ad-hoc network several of time mobile devices act as a terminal or nodes where it deal with less memory, low power storage, less central processing unit processing capability. Such devices need to optimize algorithms & mechanisms to implement the computing & communicating functions.

1.4. Security Goals for Wide Area Network (WAN) [3]
The most important thing is security issue in network infrastructure. While using WAN it also important factor to security of network connection. So it is crucial to achieve solution of problem which provide goal. Some of following goals in WAN:

- **Availability:** This is the first goal of WAN where authorized parties want to access network asset he could access all the information using network connectivity available whenever he required & wide area network have to make sure the survivability of network and it important services regardless of (DOS) denial-of-service attacks, dos can be launch at any time of any layer in WAN.[15] Ad-hoc network ensure the availability of message protection for communication network it also responsible for protect resources & terminal or nodes used for communication.ad-hoc network also responsible to control the needless processing. The key management is to manage the messages to decrease energy consumption & validate extend the network life [4, 5].

- **Authenticity:** In order to achieving availability the other important key factor is authenticity of network so it is another crucial feature & goal of WAN. Authentication is essential for most of the administrative work or tasks like to control sensor node duty cycle and network reprogramming .while the connection take place at the same time it also important for the receiver end to make sure the data or message he used posses from trusted source .so an opponent end may simply insert messages or data. Data authentication key work is to allow the receiver end to validate the data which was sent by the sender is original. Basically Stronger level of accuracy or authenticity will be provided by key authentication using concern protocol However, many of wide area network no need to ‘‘assurance’’. By the use of application protocol and system key delivery verified [6, 16].

- **Confidentiality:** Another key factor in security of data and network is confidentiality in a confidential message is a resistant to helpful its sense to an eavesdropper. Even though the routing message or information in WAN want to stay confidential, because it might be use for denial of DOS attack. So the main standard way is to keep responsive or useful data secret. These secret data is firstly encrypt with using secret key and key is share with receiver ends. Hence achieve confidentiality. Confidentiality has to be provided by small keys .to discourages a solitary shatter from compromise a big portion of the MANET ad hoc network. To establish unique keys among all pair of communicating antenna is preferable and in a security logic using an only single network with wide key [7, 17].

- **Freshness:** Freshness simply could signify key freshness & data freshness. Because of the entire ad hoc networks offer a number of forms at varying time measurements. Normally each and every people must have to make sure each message is a fresh message. So the Data freshness is directly imply with the date use in recent is fresh or not after that it ensure that none of opponent replayed old data messages [6]. On the other end A key establishment procedure between the participant have to assured that each one shared key or session key is fresh not be reused by other participant. This is also important in means cryptographic association that a key use in one has not been use for another or other association [4]. Thus in each session of transmission shared keys require to changed over the time since a key has used for (long term or session key) might be compromise for the duration of operational phases or pre-deployment of a wide area network (WAN).

- **Data integrity:** Data Integrity refers to measures and ensures that the received data in receiver end is not altered during the transition by an adversary. The services provided in data integrity are used by cryptographic and hash functions beside the number of form in encryption. The Data integrity with network security provides service implicitly.

- **Self-organization and Scalability:** In compare to General MANET (ad hoc networks) that do not place scalability inside the primary main concern. In the WAN cannot make use of a keying exchange scheme which has deprived scaling property in the sense of latency and energy cost .to maintaining a key and establishing in the WAN as an entire or used for a number of huge subset of terminal or computer nodes [6]. So when the communication take place it could be must to know the number of neighbours and what distances could be and also know power necessary to send messages along with an error rate from source end node to destination end will not be identified in advance. The same as a result we can say that it must have to the wide area network (WAN) nodes be required to be able on the way to self-organize after that carefully choose the suitable keying mechanism used for these situation [7, 18].

II. LITERATURE SURVEY

This dissertation have an idea which very simple and smooth, to reduce the complexity and transmission cost or

value over the communication network or channel or communicate take some tough call about the encryption or encoding done on message. So achieve this idea of system performance should be main task, to achieve this task have to permutes encoding vectors instead of entire body of message. But only permutes the encoding vector not enough to achieve the goal of data confidentially with better performance in throughput, encryption decryption timing, end to end delay and packet delivery ratio. For achieving these kinds of aim have to implement an additionally something important like start up key generation and this key generated randomly. After that this random generated key creates a random permutation confusion key to encrypt the message.

On other hand it's very simple to explain what we are going to do for make this system secure and healthy, Firstly transmission node its means source node permutes the encoding vector generally known as global encoding vector (GEV) instead of entire body of message with random key, to secure this random generated key mix with the confusion key and get secure entire body of message with simple and low cost encryption algorithm for mobile ad-hoc networks.

Saud Rugeish Alotaibi [9] has proposed security of MANET is turning into an inexorably complex issue. Numerous applications today, particularly military and crisis ones, depend on ad hoc wireless networks, where security prerequisites are harder to authorize than in customary systems. Securing routing makes specific challenges, since these networks have neither midway administrated secure routers nor strict strategies of utilization. The network topology is quickly changing because of node or terminal in the network being exceedingly mobile, along these lines making the nearness or nonappearance of connections. Therefore, routing is especially difficult to accomplish securely, robustly and efficiently at the same time. Security needs such as data integrity and confidentiality, authentication & non-repudiation. Or else be providing through a central server that must be enable & provide through the all nodes. Both EHARP and SEHARP are unique in the respect that no comparable proposals have been made. In addition, the secure environment approach is applied to the problem of regulating access to a hostile environment in MANET protocol. There was also a reduction in the effect of flooding in the sense of no of routing discovery packets needed to deliver data packets with different mobility speed of nodes or terminals and network size. Results also show that the ratio of no of data packet delivered to their destinations to the no of all packets generated in the networks is higher in EHARP than in the conventional AODV protocol, which is a result of choosing the longest path to the destination.

Nageswararao Sirisala et.al [10] on his research work has proposed Quality & Security are the two chief aspects in MANETs to be present addressed. Several articles comprise addressed these aspect separately. Very little encompass concerted on the deal off among quality & security of MANETs, but lost their performance. The planned technique WBTQ basically focuses on together the issue in parallel. It is provided that secure atmosphere by evaluate all node's honesty in the network in its place of with higher computational encryption algorithms with no trailing its performance. The WBTQ is basically extension of OLSR protocol while node or terminal trust values & QoS metrics is propagate in network by HELLO packets. These protocols give a feasible & flexible approach to the user in choose a superior network route by giving weight age to Quality and Trust values. The proposed WBTQ considers trust and quality constrains in route e establishment, it is expansion of OLSR protocol while the QoS & trust metrics are added as additional fields in the HELLO packet. The protocol selects the MPR nodes based on trust and band with constraints, so the routes to destination node are secure and stable. In the construction of route table the user may give more weight age either to Quality or Trust based on his requirements. All the packet formats are discussed diagrammatically in the papers that are use in the protocol. In the simulation, the proposed method performance is analyzed with respect to different parameters like delay, throughput and control overhead. The protocol WBTQ measured significantly improved results over the existing OLSR protocol.

Shayan Ghazizadeh et.al [8] in research has to suggest a safe & secure routing network protocol for MANET SADSR. Basically SADSR has focus on the authenticity of the routing network protocol messages by digital signatures which based on asymmetric cryptography. A very simple method to be proposed for issue a certificates in the offline mode procedure. In a Security aware adaptive dynamic source routing protocol (SADSR) focus on to manages the multiple routes to every destination. On this method where each of nodes in the ad-hoc network store or contains a limited trust value which is used for each other node separately. In initial step a trust value is computed for each one & every path. After that the higher trust values give first preference priority for routing the packets. The software used to approach his implementation is ns2 simulator & after the results produce then compared the performance of DSR & SADSR. There is no malicious node in the MANET network. Both have achieved the similar packet delivery ratio as compare to DSR. In the presence of malevolent nodes SADSR out performs DSR in the throughput. In the both cases Security aware adaptive dynamic source routing protocol (SADSR) introduce a sensible network load to set up the higher packet delivery ratio. A more through experimental setup is necessary to appraise the result of cryptography delays on packet latency and protocol sensitivity to parameters. Also, an enhancement for punishing selfish nodes (i.e., nodes that do not take part in routing) based on their packet delivery performance can be incorporated. Trust values for neighbours can be updated

using a method monitoring neighbour transmissions. This enhancement can lead to smaller convergence period for the trust values. Also, more experiments need to be done to measure the effects of any changes in values of parameters of the protocol and to find out what the optimal values are for different setups.

Lu Jin Zhongwei Zhang David Lai et .al [11] has proposed Another imaginative arrangement of wireless technology is MANET. A MANET is described by no established foundation & shifting topologies structure. This feature enables MANET to be sent inside numerous conditions where customary IP networks are obliged or excessively costly as far as time and assets. Unfavourably, the mobility of terminals or node renders MANETs defenceless against numerous malicious attacks. Security feature in MANETs for the most part have secures data transmission & secure routing. Nearby are as of now a few systems to protected end-to-end communication & transmission however there are constrained quantities of techniques of securing the network routing message or protocols. Due to the dynamic infrastructure and varying topology of node location in MANET, security issue needs to be carefully addressed. He focused on the securing the delivery of routing network packets & the strategy of find out the majority of secure routes. In particularly, a secure network routing protocol is carefully scrutinized. The FLSL protocol is basically based on SAODV protocol and fuzzy logic algorithm it is used to determine the secure network route with the minority probable routes. We tested the FLSL protocol on NS 2 platform and performed a number of experiments. The experiment results show the FLSL protocol can be a viable solution to MANETs. Here, we can improve the routing performance by incorporating more factors such as the node bandwidth into the security level calculation. Currently we are performing experiments on IPv6 MANETs. Another possible improvement is to extend this protocol to a situation that the nodes could move around.

Vincent Toubiana et.al [12] MANETs spontaneous and infrastructure less features failed to draw users which prefer simpler infrastructure solutions. However, scalability of MANETs could play a major part in their future deployments, but actual MANET's protocols do not cope well with scalability issue & particularly protected protocols. To manage a MANET ad-hoc network security is a very difficult face because of the natural inherent complication & incredible no of parameter must be consider. To offer a competent security management he basically focus on three major parameters which is the protected applications, the protected device capability & the connected network security. To work out this issue he proposes a technique which is known as (ASMA) Adaptive Secured Multipath for MANET Ad hoc networks. It is a flexible, scalable & it is application-oriented structure or framework .it has ability to control or manage security challenge. It does totally depend on the requirements of application & conditions of network security. ASMA is basically based on a framework or structure calls a macrograph combine together multipath routing & dynamic trust management. The macrograph framework or structure is able to calculate approximately communication security in classify to pledge to infrastructure are recognized or established. This is happen only once they contest applications security needs. ASMA give more flexibility and it offer compliance through the majority of security tools & demand routing protocols. The MANET's security tool has needed to manage through taking into relation the protected or secured applications, the network context & the secured device. Whereas maintenance of operating cost small and its limit performance degrades. Simulation demonstrates ASMA ability to safe routing protocols toward counter malevolent terminals and nodes dropping packets. In addition to this simulation results prove that the framework of ASMA provide together acceptable performances and security.

Emmanouil A. Panaousis et.al [13] in his research work has presented nature of MANET mobile ad-hoc networks which makes them an appropriate used in the perspective of an emergency used for the entire involved in emergency rescue team. A secure & adaptive routing protocol formed. The main motivation behind EMANETs is to assess & evaluate the major performance of the protocol through contrasting it & some other generally utilizes routing protocols intended for MANETs. at last demonstrate operating cost acquainted owed by security reason & to assist secure ad-hoc network communications between lightweight devices.

Saud Rugeish Alotaibi [14] has proposed security of MANET is turning into an inexorably complex issue. Numerous applications today, particularly military and crisis ones, depend on ad hoc wireless networks, where security prerequisites are harder to authorize than in customary systems. Securing routing makes specific challenges, since these networks have neither midway administrated secure routers nor strict strategies of utilization. The network topology is quickly changing because of node or terminal in the network being exceedingly mobile, along these lines making the nearness or nonappearance of connections. Therefore, routing is especially difficult to accomplish securely, robustly and efficiently at the same time. Security needs such as data integrity and confidentiality, authentication & non-repudiation. Or else be providing through a central server that must be enable & provide through the all nodes. Both EHARP and SEHARP are unique in the respect that no comparable proposals have been made. In addition, the secure environment approach is applied to the problem of regulating access to a hostile environment in MANET protocol. There was also a reduction in the effect of flooding in the sense of no of routing discovery packets needed to deliver data packets

with different mobility speed of nodes or terminals and network size. Results also show that the ratio of no of data packet delivered to their destinations to the no of all packets generated in the networks is higher in EHARP than in the conventional AODV protocol, which is a result of choosing the longest path to the destination.

III. ENCRYPTION ALGORITHM BASED ON PERMUTATION SCHEME (PPE) ON PROPOSED DYMO

The main concept of the scheme, called permutation scheme, is that only GEVs are permuted in preference to the entire packets at the supply. This makes sufficient confusion for an adversary to find GEVs in an effort to get significant records. As discussed above in this chapter permutes the GEVs has great move to make proposed mechanism more perfect and more efficient it has reduces huge amount of complexity.

On the opposite hand, as the header length or duration won't be long sufficient for permutation to attain enough security, we additionally propose using random encryption key on message to in addition growth the safety of the proposed scheme towards antagonistic attacks.

As the below depicted figure 2 shows the proposed permutation mechanism on DYMO routing protocol follows some steps:

1. Start the permutation scheme.
2. Initialize the source message i.e. (original message not encrypted message) m_1, m_2, $m_3 \ldots m_h$ (Total number of messages are h). The length of individual message n – h.
3. Each of messages is padded with the unit vector as the header. Due to padding it behaves or performs the linear combination of data packet and also generates the individual or independent data packet and number of independent packet is h.
4. After the performing of linear combination to generate the individual or independent data packet, permutation scheme will perform or conduct the encryption on the individual data packet (total number of data packets h).
5. In this permutation mechanism firstly permuted the GEVs based some permutation key k.
6. At last but not the least done random key encryption on message of DYMO protocol.

This paper proposed something important regarding security to mobile ad-hoc network or communication network. Dimension of statistics has been playing a major role for secure communication through mobile ad-hoc network, in this secure transmission permutation that is partially gives a great idea without any complexity and this mechanism using some important notation which introduce or define the partially permutation encryption mechanism shows in the table 1.

Figure 1: Permutation Encryption Mechanism

Symbol	Explanation
X_i	Source Packet
X	Vector Matrix of Source Packets
H	Number of Message, Permutation Length
Y (e)	Coded Packet Carried on Link e
β (e)	LEV of Link e
g (e)	GEV of Link e
G	Global Encoding Matrix
A	Sequence of GEVs
K	PEF Key
C	Cipher Text
D	Data Generation
f (h)	Function Used for Confusion Key
k'	Confusion Key for Each Data Generation

An ordinary MANET scenario involves a source node, intermediate nodes, and sinks nodes. Figure 2 shows the permutation schemes on coded messages for the routing protocol as well as Figure 3 depicts the data transmission in a MANET based totally at the proposed permutation encryption scheme and community coding and the permutation encryption scheme is most effective done at the source nodes for encryption and on the sink nodes for decryption, and the intermediate nodes carry out recoding of the message packets.

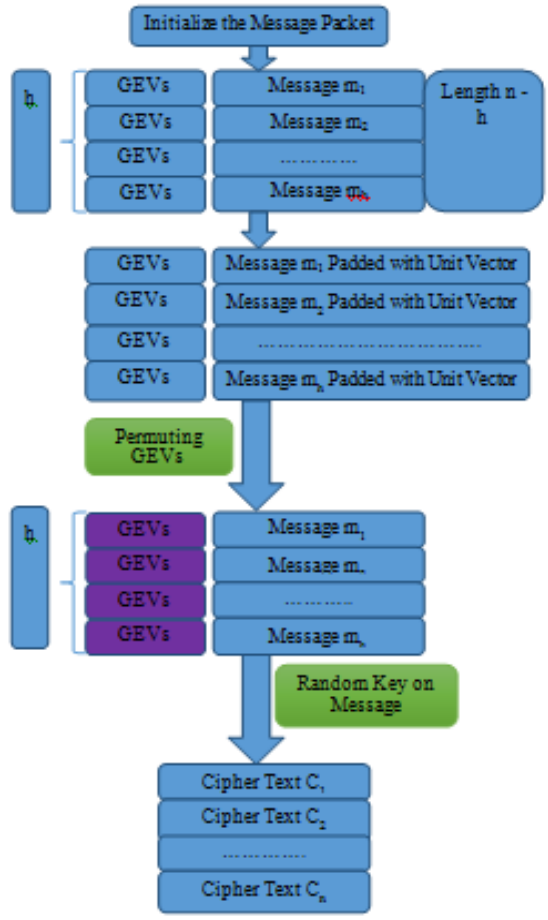

Figure2: Permutation Scheme on (Proposed DYMO Protocol) Coded Message

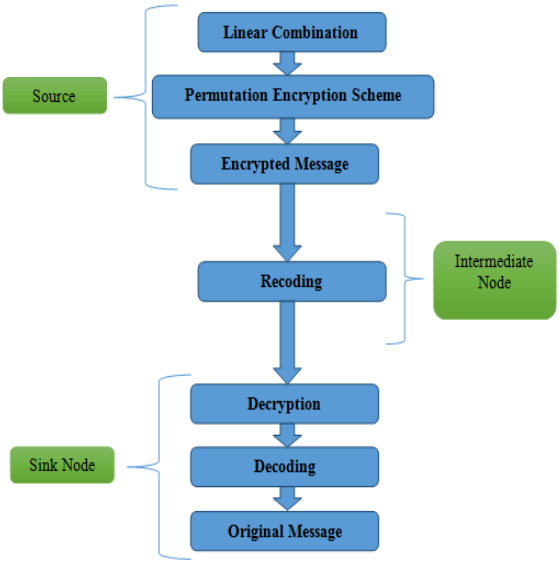

Figure 3: Secure Data Transmission Stages (MANET)

3.1 Generating Algorithm of Dynamic Random Key

In a scenario where source needs to transmit big statistics quantity from one node to different nodes, supply ought to first divide data into generations and use perturbing key on every records generation. If a single perturbing key is used within the path of transmission then there is a danger that this key might be disclosed, so as to result in compromising safety of the whole statistics extent. This is known as single technology failure.

Assume the subsequent steps are achieved by way of source on i^{th} information era $\boldsymbol{D_{Gi}}$, and key $\boldsymbol{k_i}$ is generated.

1. Randomly pick $\boldsymbol{h}$ positions among information generation $\boldsymbol{D_{Gi}}$ which might be referred to as perturbing key.
2. Corresponding to information generation $\boldsymbol{D_{Gi}}$, key $\boldsymbol{k_i}$ is calculated in keeping with Algorithm 2.
3. Encrypt $\boldsymbol{D_{Gi}}$ primarily based on $\boldsymbol{k_i}$ and the encrypted facts or info or data generation is dispatched or send from supply or source node to all participant nodes which can replace or update key.

Dimensions of statistics used for each of several possible ways in which a set of value of dimensions of statistics things can be ordered or arranged (commonly known as permutation) characteristics for each global encoding vectors and also generation of secret dynamic random key explain by the algorithm 1 which has listed below:

Algorithm 1:

(1) ArrayK[] /∗ size m∗/
(2)Function Key Gen (integer m)
(3) Initialization (m)
(4) For i ← 1 to m − 1
(5) ψ ← rand() /∗ between i to m∗/
(6) K[i] ← perm (ψ)
(7) End for
(8)Function Initialization (integer q)
(9) For a ← 1to q
(10) K[a] ← a
(11) End for

Algorithm 1 steps written as follows;

Step 1: First step of this process algorithm is declaring the array key size m.

Step 2: To key generate get the key size its (Function Key Gen) and define argument.

Step 3: Initialize the function of proposed system used to be call key size m.

Step 4: Taking any random value between i and m and this value stored in ψ.

Step 5: By taking the random value between i and m, permutation function treats this value as a seed to generate a new value as key [i].

Step 6: This processes will end until loop execute m – 1 times.

Step 7: Initiate system function, here the function has a value from a to q.

Step 8: There is important fact the value of a initiate from one and a is basically store as a key [a].
Step 9: Loop end at q.
Traditional cryptographic method like AES for quit-to-cease encryption cannot be used due to the limited resource skills of MANETs. This work contributes to generate lightweight encryption key as proven in Algorithm 2, which introduces a random quantity and updating key for each information era to enhance protection and decrease computation and communicate overheads from supply to destination in MANETs.

IV. SIMULATION RESULTS

In this section, we discuss simulation results and various parameters.

4.1. Mobile Node Parameters

It would be helpful to check the example scripts in ns/tcl/ex on wireless networks (for ex: wi-fi.Tcl). This should give a few concepts of the special parameters that want to be configured for a normal simulation. A listing (table 2) of all parameters is given under for reference.

Table 2: Network Mobile Node Parameter

Sr. No.	Parameter	Value
1	Channel Type	Wire Less Channel
2	NS-2 Version	NS-2.35
3	Radio Propagation	Two way Ground
4	Number of Nodes	50
5	Routing Protocol	E-DYMO
6	Protocol MAC	802.11
7	Interface Queue Type	Queue/Drop-Tail/Pri-Queue
8	Network Interface Type	Phy/Wirelessphy
9	Link Layer Type	LL
10	Antenna Model	Omni Antenna
11	Frame Size	512
12	Mobility Model	Random Way Point
13	Coverage Radius	71 m
14	Shadowing	0db
15	Frequency Band	2.4 GHz
16	Sending Rate	1 frame every 250 ms
17	Bit Rate	54 Mbps

4.2. Topology Parameters

These are the configuration parameters for the topology structure, like the dimensions of the grid, wide variety of nodes gift and so on. A list of they all is given underneath for reference. One can once more refer to the sample script above for an example.
X - Size of the topography
Y - Dimension of the topography
Number of nodes other parameters are,
Total simulation time, and
Trace document name

4.3. Scenario File

Construct person node movements are viable but bulky for a simulation going for walks on the order of 200 seconds and more. For ease of use, a script has been furnished which generates those actions automatically in a separate document. I name this the scenario document. To generate this, use the set script found in ns/indep-utils/cmu-scen-gen/ listing. The nodes move round with a pace randomly selected among zero and max speed. Each node selects a vacation spot and a pace and moves towards the destination. Once it reaches there, it pauses for a time pause time, after which chooses any other destination to move to.

4.4. Traffic pattern file

Further, we require site visitor's generators at nodes, and sinks at the locations. The creation instructions for these site visitors' sellers are entered in a separate document, the traffic sample record. An example configuration is given beneath:

```
settcp_(zero) [$ns_ create-connection TCP/Vegas $node_(0) TCPSink $node_(1) 0]
    tcp_(zero) set window_ 32
    $tcp_(zero) set packetSize_ 512
    $tcp_(0) set v_alpha_ 2
    $tcp_(zero) set v_beta_ 2
    set ftp_(0) [$tcp_(0) attach-source FTP]
     $ns_ at 1.0 "$ftp_(0) start"
```

Once most of these parameters are configured, the simulation may be run. The maximum important record finally ends up within the trace report. The occasions logged but are at a completely microscopic level, giving data about each degree a packet traces from source to destination. This file needs to be filtered to achieve combination results like throughput, utilization and many others.

4.5. Comparison Performance Analysis

In table 3 represent the comparative performance of throughput parameter for the given Proposed DYMO and Encrypted DYMO routing protocol.

Table 3: Throughput value of Encrypted-DYMO (E-DYMO) protocol and Proposed DYMO Protocol with increasing number of nodes

Number of Node	Throughput Proposed DYMO	Throughput EncryptedDYMO (E-DYMO)
10	314.061	285.51
20	276.184	240.16
30	538.780	489.80
40	514.116	428.43
50	468.809	407.66

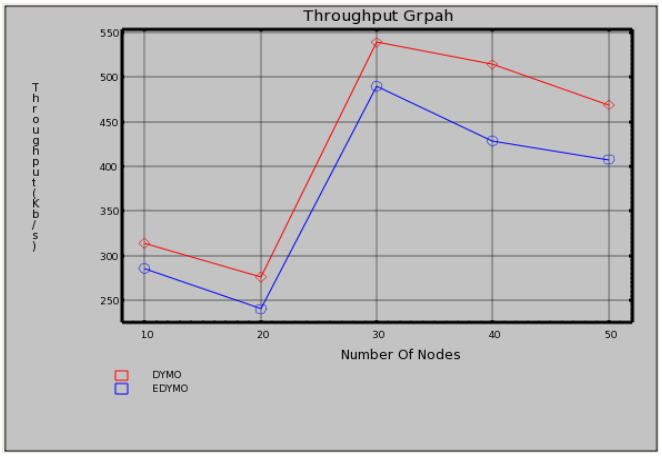

Figure 4: Compression of throughput of Proposed DYMO and E-DYMO

Here, figure 4 shows the comparative study of throughput according to number of number of nodes of Proposed DYMO and EDYMO routing protocols.

Table 4: PDR value of Encrypted-DYMO protocol and Proposed DYMO Protocol with increasing number of nodes

In table 4 represent the Packet Delivery Ratio (PDR values) according to increasing number of nodes (10 to 50) of Encrypted-DYMO and Proposed DYMO routing protocol.

Number of Node	PDR Proposed DYMO	PDR Encrypted DYMO (E-DYMO)
10	0.517	0.47
20	0.371	0.37
30	0.583	0.55
40	0.698	0.64
50	0.342	0.32

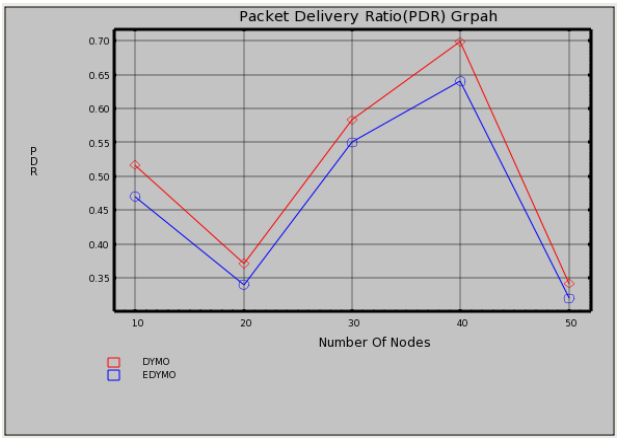

Figure 5: Shows Graph between number of nodes and PDR of Proposed DYMO and E-DYMO

Here, figure 5 represent the packet delivery ratio graph between proposed DYMO and E-DYMO routing protocol,

Table 5: End to End Delay value of Encrypted-DYMO (E-DYMO) protocol and Proposed DYMO Protocol with increasing number of nodes

Number of Node	EtE Delay Proposed DYMO	EtE Delay E-DYMO
10	193.275	212.39
20	98.620	103.81
30	99.700	108.37
40	107.309	116.64
50	113.449	120.69

Figure 6: Shows Graph between number of nodes and EtE Delay of Proposed DYMO and Encrypted-DYMO(E-DYMO)

In above table 5, we represent the end to end delay value of Encrypted-DYMO protocol and Proposed DYMO protocol according to increasing number of nodes as well as we shows that the graphical representation of above table for end to end delay in figure 6.

V. CONCLUSION

We have used a partial permutation encryption algorithm for proposed DYMO. Instead of permuting the entire packet as in the previous P-Coding method, the encryption scheme permutes only GEVs which decrease the computational complexity; it is efficient encryption algorithm in terms of energy, computation, and cost. The encrypted DYMO routing protocol gives more security against various attacks; we analyzed encrypted DYMO routing protocol by taking into account different parameters: throughput, PDR and end to end delay. The Encrypted DYMO (E-DYMO) more secures than other routing protocols as well as enhances the security of proposed DYMO.

REFERENCE

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

[2]. C. Siva Ram Murthy and B. S. Manoj "ad hoc wireless network, architectures and protocol.

[3]. Perkins, Charles E. Ad hoc networking. Vol. 1. Reading: Addison-wesley, 2001.

[4]. B. Dahill, B. N. Levine, E. Royer and C. Shields. Aran: A secure routing protocol for ad hoc networks. Technical Report UMass Tech Report 02-32, University of Massachusetts, Amherst, 2002.

[5]. L. Zhou, Z.J. Haas, Securing ad hoc networks, IEEE Network 13 (6) pp.24–30, 1999.

[6]. A. Perrig, R. Szewczyk, V. Wen, D. culler, J. Tygar, SPINS: security protocols for sensor networks, in: Seventh Annual ACM InternationalConference on Mobile Computing and Networks Mobicom 2001), Rome, Italy, July 2001.

[7]. D. Carman, P. Kruus, B. Matt, Constraints and approaches for distributed sensor network security, NAI Labs T.R. #00-010, 1 June 2000.

[8]. Shrestha, Ashish, and Firat Tekiner. "On MANET routing protocols for mobility and scalability." In Parallel and Distributed Computing, Applications and Technologies, 2009 International Conference on, pp. 451-456. IEEE, 2009.

[9]. Johansson, Per, Tony Larsson, Nicklas Hedman, Bartosz Mielczarek, and Mikael Degermark. "Scenario-based performance analysis of routing protocols for mobile ad-hoc networks." In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pp. 195-206. ACM, 1999.

[10]. Sethi, Srinivas, and Siba K. Udgata. "Scalable Cluster Based Ad hoc On-demand distance vector routing protocol for MANET." In Wireless Communication and Sensor Networks (WCSN), 2010 Sixth International Conference on, pp. 1-6. IEEE, 2010.

[11]. Park, V and Corson, S "Temporally - Ordered Routing Algorithm (TORA) Version 1 Functional Specification". IETF MANET Working Group, 2001.

[12]. R. Dube, C.D. Rais, K-Y.Wang and S.K. Tripathi, ―Signal Stability-Based Adaptive Routing (SSA) for Ad-Hoc Mobile Networks‖, IEEE Personal Communications journal, February 1997.

[13]. Gupta, Jyoti. "Survey on Different Approaches of Detection of Gray Hole Attack in MANET." 2017.

[14]. Johansson, Per, Tony Larsson, Nicklas Hedman, Bartosz Mielczarek, and Mikael Degermark. "Scenario-based performance analysis of routing protocols for mobile ad-hoc networks." In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pp. 195-206. ACM, 1999.

[15]. Singh, Ajay Vikram, and Moushumi Chattopadhyaya. "Mitigation of DoS attacks by using multiple encryptions in MANETs." In Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2015 4th International Conference on, pp. 1-6. IEEE, 2015.

[16]. Shengming Jiang, Dajiang He and Jianqiang Rao "A Prediction-Based Link Availability Estimation for Routing Metrics in MANETs", IEEE Transactions on Networking, Vol. 13, No. 6, December 2005.

[17]. A. Perrig, R. Szewczyk, V. Wen, D. culler, J. Tygar, SPINS: security protocols for sensor networks, in: Seventh Annual ACM InternationalConference on Mobile Computing and Networks Mobicom 2001), Rome, Italy, July 2001.

[18]. Gowda, Sumati Ramakrishna, and P. S. Hiremath. "Review of security approaches in routing protocol in mobile adhoc network." International Journal of Computer Science Issues (IJCSI) 10, no. 1 (2013).

Authors Profile

Mr Mukesh Dixit pursed Bachelor of Engineering from RGPV University in 2005 and Master of Technology from RGPV University in year 2010. He is currently pursuing Ph.D. in Mewar University Chittorgarh. He has published more than 20 research papers in reputed international journals and conferences.His main research work focuses on Wireless Network, Routing Algorithms and Network Security.

Dr. Sarvottam Dixit is an, M.E. (computer Science), Ph.D. (Material Science) from "Agra University" (now called "Dr. B. R. Ambedkar University"), India and has done Post Doctoral Research work in at TIFR, Mumbai., . He is currently working as Professor in Department of Computer Science & Engineering, Mewar University of Chittorgarh (RJ). He is a member of various computer societies. He has published more than 35 research papers in reputed international journals and conferences. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, and Computational Intelligence based education. He has 15 years of teaching experience.

Dr. Ajay Kumar Sachan, had completed his Ph.D (Computer Science & Engineering) from Rajeev Gandhi Technical University, Bhopal in 2007. He has published more than 35 research papers in National & International Journals. He is a member of various computer societies. His main research work focuses on Routing Algorithms, Network Security, MANET; He has more than 21 years teaching & research experience. Presently working as Director in LNCTS College, Bhopal

.

