Evaluation of Hybrid Security Mechanism for AODV in MANET

[1]Shelbala Solanki, [2]Anand Gadwal
[1,2]Dept. of CSE, Sagar Institute of Research and Technology Indore, MP, India

Abstract
Mobile ad-hoc network is used for communication between the short range devices without having any infrastructural support. Here the devices directly exchange the data and routing information between neighbourhood devices which was there in defined range. Such network lacks with centralized controls and hence the information regarding the nodes leaving the range or nodes coming into the ranges are maintained by each node in their routing tables. In some situations, dynamic topologies and heavy movement causes security degradations because to verify the authenticity of each node participating in communication is not possible. Thus to have effective authentication and confidentiality is became a challenging task. This work uses RSA public key cryptosystem and SHA-I as digital signature for verification of hash codes of identity information's. It is capable of handling both the information of data and control packets. After the robust analytical evaluation and quantitative measurement the effectiveness of the tool and its workability is verified.

Keywords
Ad-Hoc Network, MANET, Secure AODV, Confidentiality, RSA, Authentication, Digital Signature (SHA-I);

I. Introduction

Ad-hoc network represents the group communication handling between the nodes in community exchanging data and control messages without using any infrastructural entities. The relationship establishes and sustains the characteristics simplest considered and strongly imparted communication for nodes in a defined range. Here each node will function like a router which helps the conversation protocols without any centralized controls and known as as autonomously organized. Even though the above characteristics of ad-hoc community is adaptive and easy in nature. It can take distinctive forms and has surprisingly variable movable device characteristics together with power and transmission conditions, visitor's distribution variations, and load adjustments [1]. Formerly the data packets may be provided effective protection without difficulty using some of conventional security primitives but serving same for manipulative or control packets is quite complex. The control packets are also known as routing packets follows certain rules like sending requires immediate acquaintances with its nearby nodes, it should be processed and can be modified processed, probable modified, and resent to the source. Managing the proper implications of the security is taken as major process of applying the protection among the unreliable networks.

MANET manages the security consideration by maintaining their security; we call them "Security Parameters". Being unaware of these parameters may cause a security approach useless in MANET. Generally there are two important aspects in security: Security services and Attacks [2]. Services refer to some protecting policies in order to make a secure network, while attacks use network vulnerabilities to defeat a security service. Each security approach must be aware of security parameters as shown in fig. 1. All mechanisms proposed for security aspects, must be aware of these parameters and don't disregard them, otherwise they may be useless in MANET.

- **Network Overhead:** This factor refers to count of control packets generated by security mechanism towards robust protection features. But the shared wireless media with higher number of control packets may easily lead to collision or congestion. Packet misplaced is one the consequences of congestion and collision. Therefore, high packet overhead increases packet lost and the number of retransmitted packets. This will easily wastes nodes energy and networks possessions [3].
- **Processing Time:** Each security approach needs time to detect misbehaviours and eliminate malicious nodes. Appropriately MANET's supports dynamic topology used to establish routes between two different nodes changing their position due to high mobility. Therefore, security approaches must have as low as possible processing time in order to increase MANET flexibility and avoid rerouting process.
- **Energy Consumption:** In MANET nodes have limited energy supply. Consequently, optimizing energy utilization is extremely challengeable task in MANET due to their limited battery power supplies. Larger be the consumption fewer will be the network lifetime.

A. Types of Attacks

1. Network Layer Attacks

This section lists and gives brief description of the attack pertaining to network layer in the network protocol stack.

- **Wormhole Attack [4]:** A Wormhole attack is performed by more than one attacker. Here the environment is composed of two attackers and a wormhole tunnel used to mislead the routing. It is initiated by an attacker which creates a direct link, referred to as a wormhole tunnel, between them. An attacker receives packet at one location in the network and tunnels them (possibly selectively) to another location in the network, where the packet are resent into network [20]. This tunnel between two colluding attackers is referred to as a wormhole. If proper mechanisms are not functioning to defend the network in opposition to wormhole attacks, nearly all of the existing routing protocol for MANET (mobile ad hoc network) may fail to find valid routes.
- **Black Hole Attack:** In mobile ad hoc network black hole attack is a type of DoS (denial-of-service) was the router in control would discard the packet instead of replying for them. The blackhole or malicious node will always drops the genuine communication packets from the network nodes. It shows the behaviour of shortest route and when the communication gets started then the whole characteristics of the node is been changed to some uncertain behaviour. Primary, the node exploit the ad hoc routing procedure, such as AODV, to broadcast itself as having valid route to a target node, even during the route is forged, with the intent

of intercepting packets [5]. Subsequently here the node consumes the intercept packet transmitted by the sender. Black hole attacks in AODV protocol routing level can be classified into two categories: RREQ black hole attack and RREP Black hole attack [21].

- **Byzantine Attack:** Here, a compromised transitional node or a set of attacked nodes works in combination to create routing loops, routing packets on non-optional path and selectively dropping packets [6]. Byzantine failures are hard to detect. The network would appear to be working in general in the perspective of the nodes, though it may essentially be exhibit byzantine activities.
- **Information Disclosure:** An attacked node with fewer controls may loss the confidentiality of information to some malicious node in the network. Such information may include information regarding the network topology, geographic location of node, or optimal route to authorized node in the network.
- **Resource Consumption Attack:** In this attack, a malicious node tries to consume/waste away resource of other node present in the network. The resources that are targeted are bandwidth, battery power and processing capabilities, which could be of limited nature in ad hoc wireless networks.
- **Routing Attack:** There are several types attacks mounted on the routing protocol which are aimed at disrupting the operation of the network.

2. Transport Layer Attacks

This section discusses an attack which is specific to the transport layer in session hijacking. In this type of attack the adversary node takes the communication control from intermediate session of two nodes. Here the authentication procedures had started at the start of communication sessions and once it is been established then the malicious node take the benefits from unintended session tracking and other malware activities.

3. Application Layer Attacks-Repudiation

In simple term, repudiation refers to the denial or attempted denial by a node involved in a communication of having participates in all or part of the communication. Non-repudiation is one of the significant necessities for a security protocol in any announcement of network.

4. Multi-Layer Attacks

In this type of attack the network resources are affected by attacker at multiple layers during communication.Some common examples are DoS (Denial of service) and impersonation (IoP) etc at multi-layer stack.

II. Motivation

There are so many severe attacks that can easily be launched even in networks with confidentiality and authenticity. Malicious nodes usually targets the routing control messages related to routing information. Various methods and techniques used for the detection and prevention of attacks along with their advantages and drawbacks are also discussed. This work analyses the effect of various attacks that can be prevented using the hybrid security mechanism formed by integrating the cryptosystems along with the digital signature. Finally we have proposed a new, efficient algorithm for AODV protocol and compare some factors end-to-end delay, throughput, packet delivery ratio etc. In ad-hoc network each node has facilitative features t help the node movements along with properly coordinated directions. Somewhere it generates the security loops for the user. It was one of the most important factor towards getting the better security solutions in ad-hoc network. It should also be developed in light weight manner because security rules are having higher burden towards calculating the authenticity and maliciousness for each participating nodes. The mobility based nature of MANET invites the attacker with high attraction easy environments for affecting the network resources. Some of the measured surveys shows the nature of attacks affecting the throughput, performance and the network lifetime. Sufficient research has been made towards developing the attack resistant surface for defending the network resources. Hard works are putting to get better the network safety mechanism for smooth complex operation against co-operative black hole assault.

III. Contribution

In this work implementation and analysis of authentication and confidentiality attack prevention and detection for mobile ad-hoc networks with emphasis on deployment on simulators for studying the real effects of the suggested approach. The suggested solution and the discovered area directs towards customization of the end user network application with higher security and better protection towards data and control packets.To solve the above problem of effective detection of wormholes some parameters like delay per hop (DPH) and TTL values are used. Apart from the above description the contribution involves:

1. Identification of the best suitable approach towards encrypting the packet content and authenticating the user's information using digital signatures with particular arrangement of hardware components and scenarios.
2. Evaluating the approach on different attack situations based on the nodes configurations and parameters of throughput, PDR and routing overhead.
3. Dynamic behaviour handling and less resource constraints with mobility based modifications
4. The work also provides the identification of the usable configuration methods, built-in functions and limitations of hardware communication platform, which can influence the opportunity of the Wormhole detection.
5. The work also provides an implementation analysis of the suitable and reliable communication protocol.
6. The simulations of QoS based traffic scenarios brought out the behaviour and priority details in multi-hop network.

IV. Background

Mobile ad-hoc network (MANET) is a dynamic type of wireless communication network with mobility support due to their changing topological nature. Nodes are portable in nature and regularly changes their positions requires high configurations. It will also executes the request with minimum resource consumptions like battery and bandwidth. As MANET is not having any central administrative controls and the source and destinations will communicate s using multiple intermediate hops. Here the nodes can change their positions needs to be updated with their routing tables. It is quite complex to manage their authenticity. Hence the attacker keeps the track of activities to get malicious control over the network. MANET shows high vulnerability to various attacks having intentionalcharacteristics to affects the formal performance by dropping or changing the routing procedures. Mainly these operations are performed from some non-trusted nodes.

There are several attack to which MANET provides open surface due to its nature. Weneed to explore them for having in depth

knowledge of security loopholes by which some feasible and effective solution can be derived. In way to do that, this work puts an approach and its analysis which works towards making the things more effective for the detection process. Attacks perform various malicious tasks by misdealing the routing information, scanning the confidential data behind it or dropping the complete message intentionally by the malicious users or node. It will drop the packets of different magnitude and route generation. It is the most serious threat for the MANET and can't be detected easily.

A. Security Considerations

MANET requires high end configuration for security due to its dynamic nature like for some critical applications. As it was an open environment then we have to impose some considerations with higher requirements. We have limited resources with mobile devices due to their cost and size. Security is of critical importance in many networks, especially in likely applications of MANETs. There are further security challenges that need to be addressed in later versions of MANET routing codes. Networks must provide confidentiality, authentication, integrity, non-repudiation and availability [2].

Confidentiality is the ability to guarantee the privacy of the data transferred. In wired networks an eavesdropper has to be in the path between the source and destination of the communication entities in order to "sniff" on the transit traffic. Wireless links, however, can suffer from multiple points of attack as eavesdroppers will get the transferred data even though it was not on the path of transit traffic which will have its own radio frequency for communication. Each operation requires variable data for conducting their operations and hence they require routing information or confidentiality can be disclosed to mobile entities participating in communication.

B. Description of RSA Algorithm

RSA is one of the first practical public-key cryptosystems used for providing safe and reliable means of data communication over the protected channel. Main concept behind the protection is the randomness of the key and its difference for sender and receiver. The cryptosystem is parted into two major areas i.e. private key cryptography and public key cryptography. With this work we are mainly focusing towards providing security using public key cryptosystem. Mainly the cryptosystem here developed is RSA. In this algorithm the asymmetric nature is developed using factor solution for product of two large prime numbers.

A RSA cryptosystem user will generates and then releases public key based on two large auxiliary values based prime numbers. These numbers or their factored solution must be keep secured or protected before decrypting the message. Those who are using this cryptosystem must encrypt their message using the public key published from their public key register. If the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.

RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key.

C. Description Hash Algorithm

Hash is the well-known algorithm used for authentication and providing the better protection against the attacker. Here the digest generation plays a major role in serving the goal. It can be considered as cryptographic approach but with different type of protection. It is widely use in generating the digital signatures and hence used in combination with the SHA and MD algorithms. It mainly follows the one way generation policies due to which it breaking is made very difficult and used most.

It can also be used for password protection using HMAC and serve higher degree of confidence on security primitives. Another alternative is MD5 and SHA-1 which takes variable size input and produces fixed size length output termed as digest.

V. Related Study

This section covers the direction of some previous work made with similar domain. We have found the various research articles covering the similar type of issues with considerable differences in their outputs and analysis. Keen observation in the field of security we have found that it was the most common and tedious task to serve better protection in communication over MANET. The existing security controls can fabricate the routing information maliciously to affect the normal operations of MANET. But still there are some approaches and articles which were fruitfully directing our work to be completed efficiently. These are covered as related study in this section.

In the approach given with [12], author mentions the problems associated with configuring the network with ad-hoc nature. It covers the problems came in communication without any centralized controlling authority or say infrastructure.Authentication process for the nodes in the network it ought to be assigned the codes from its unique ranges. For making such community protected against the diverse network vulnerabilities there need to be some safety mechanism available with them. The paper cautioned a singular safety mechanism for the VASM protocol primarily based on zero information technique. Here a hash function has minimized execution time which tells the light weight nature of this scheme. The approach uses the mixture of the hash and SHA-I method.

Another article puts a light on MANET security given with the paper [13] and provides test implementation for cellular computing based communications. It works with none specific infrastructural necessities and serve the purpose of high end security needs. The paper addresses the issues of the MANET with fewer administrations and lighter mobility support. The work makes of serving the goals for the OLSR protocol using comfortable hash algorithms (SHA-1) and AES respectively. At the evaluation point of the view the approach seems to provide the reduced computation time with lower complexities of the system. It also gives a light weighted solution.

The paper [14] covers some of the security objectives for the OLSR and STAR routing protocols for pretending the data dropping and malicious node detections. The paper deals with the IPSec mechanism for the MENET. The performance is decrease if malicious node is not present in the network, because overhead of IPSec protocol is considered with the suggested system in paper. In this paper the author proposed the composite technique to limit the packet losing by means of malicious nodes detection. Here the given community uses IPSec with OLSR and STAR routing. It also puts a light of comparison with existing approach in absence of IPSec protocols.

There are some other approaches suggested with the literature which works on improvising the traditional security control of MANET using IPSec. One of such approach is IPSec-LANMAR given with [15]. It works with the propagation model using two basic characteristics path loss and shadowing is presented. The IPSec-LANMAR gives a strong impact on the performance of a protocol because the propagation model determines the number

of nodes within one collision domain, an important input for contention and interference. The simulation result indicates that open propagation model along with practical implementation with an IPSec-lanmar routing protocol outperforms with existing model. The designed experiments are carried out with network simulator.

The paper [16] suggested a solution as an extension to AODV called Secure AODV (SAODV). Mainly the security in MANET is served here using IPSec which was discussed earlier. The work assures that the IPSec implementation can use as a selector the TCP and UDP port numbers. Network communication contains two types of packets data and control. Thus the security mechanism must allow the control packet directly without change and the data packet is verified using cryptographic primitives. The information relative to the hash chains and the signatures is transmitted with the AODV message as an extension message that will be refereed as Signature Extension.

Carrying forward the above work for providing the security to MANET the paper [17] gives a protocol named as SNAuth-SPMAODV. It provides a robust way of defence against Denial of Service (DoS) attacks. It protects both routing information and data message at network layer in MANET. Also the protocol works towards multipath discovery between the sender and receiver without any additional packets for authentication. It combines the IPSec and SNAuth. It implements the basic functionality of IPSec for MANET such as ESP and AH. While evaluating the approach it gives higher results in term of processing efficiency, routing load and simulation time.

The paper [18] works towards improving the above authentication for MANET specifically for multicast packets security. Most of the times multicast allows transmission of a single packet to many users, possesses a potential danger of malicious activities which consumes the resources and affects the normal working. Suggested AuthMAN is a scalable and lightweight mechanism to address the problems of authentication in multicast mobile ad hoc networks. The suggested approach of AuthMAN uses time-delayed key disclosure along with symmetric cryptography to achieve authenticated broadcast in defined range. AuthMAN uses time as an asymmetry property and it requires sender and receiver need to be time-synchronized.

The paper [19] presents an IP based auto configuration mechanism for MANET. It focuses on developing a security solution with dynamically changing topologies and lack of infrastructures. Thus, security is also a main issue in address allocation. To develop a framework for Auto and safe allotment using some addressing mechanism. In MANET each node creates with public key cryptography and will have a unique identity assigned using IP addressing. Here the auto configuration is used in absence of centralized administration.

VI. Proposed Work

The proposed work will give a novel approach which enables the trusted communication in a secure manner over the non-trusted nodes zones of ad-hoc networks. In MANET the nodes and their topologies are dynamically changing, thus to verify their authenticity and malicious behaviour is not possible most of the time. But there is away by which the communication and transmission process can be made more secure than it was previously developed. This work will give a robust solution embedded with AODV which makes a guaranteed secure communication using digital signature (SHA-I). It serves the complete requirements of the MANET as it was lightweight, consumes fewer resources and is effective. The process starts with the initiations of route discovery. The suggested scheme give a generic way of communication is a secure manner with lower range radio signals. The nodes participating in such a communication is not aware about the intermediate operations of the encryption and cryptosystem. The work had also make the security schemes clear and starts evaluating them in a default mode. The approach is able to perform both authentication using digital signature and serve confidentiality using cryptosystem.

The source S sends the RREQ message to its neighbour with a destination id. The neighbour node checks weather the id belongs to its own, or its subgroup or someone else known by him. If all the matching is not found then it is further forwarded to next intermediate nodes. Once the destination is found in this way then the destination node separates the type of data packets and control packets available with the request. It is segregate into two categories: Mutable information and non-mutable information. The non-mutable information something related with the source and its data and the mutable information is that which could be read out by the intermediate nodes and destination such as hop counts. This non mutable information is digitally signed with the destinations signature and embedded with the non-mutable information in a RREP packet. Now, each intermediate node receiving this RREP packet will verifies the destinations signature from its neighbour table. If the signature is matched then only the packet is transmitted to next node from where it reaches to source S.

If the signature is not matched at the intermediate node then it was dropped by them. Finally the reply reaches the source where it first matches the signature of its neighbour then the later ones are matched and if the first ID is not matched then it was dropped by source itself.

Now, the source knows the complete path and signed information for each intermediate nodes. The source selects the key for its respective intermediate nodes for transmitting the data to destination D. The key is gathered either from its neighbour table or calculated from its signature. The sender source encrypts the data containing in the packet by RSA cryptosystem which perform encryption using the public key of source S. The destination receives this and decrypts the data using its private key. Once the data decryption is successfully performed by the receiver or destination after verifying the data and all its information's integrity the success acknowledge message is revert back to the sender source S. Source verifies and confirms the data transmission only after getting this success ACk message. If this message is not received then the next time repeat transmission will be performed from the different routes. Thus the work applies an enhancement over existing protocol which allows the routing using shorter directional routes with reduced delays, and longer battery life better than existence works.

VII. Algorithm

```
Algo SHA (Node [], N)                    // SHA is algorithm name
which define N number of nodes
{
Declare RREQ, RREP, S,D, SIGN, DID. Data, Ack, E_Data     //
Source, Destination, RREQ, RREP
                                  //Signature key and Destination Id  is
declared
Repeat i =1 to N
        {
           S->Send (RREQ, Node [i+1])
           Node [i+1] ->Receive (RREQ, S)
         If (D.DID! =Node [i+1].ID)
```

```
        {
                Repeat until Node [i+1].ID==D.DID
                {
                Node [i+1]->Verify(SIGN, Node[i+2])
                E_Data->Cryptosystem (SIGN, Data)
                Node [i+1]]->Forward(RREQ, Node[i+2])
        }
        }
        Else
                {
                  D->Send (RREP, S)
                 D_Data -> Cryptosystem(SIGN, E_Data)
S->Receive (RREP, D)
                S->Send (Data, D)
                D->Send (Ack, S)
                }
        }
Exit
}
```

VIII. Result Evaluation

For showing the practical feasibility of the proposed approach the work is implemented on well-known simulation tool NS2. To prepare simulation for desired network utility the following given network setup is provided. Using TCL script the network scenario is created then Simulation is executed. And by using AWK file RREQ packets send, received is captured and also used for the remaining energy of the nodes. When the simulation starts then trace file and nam file generated. Fig shown below is the scenario of the Wireless mobile ad-hoc network with thirty nodes.

Table 1: Network Setup

No of nodes	50
Radio-propagation	Propagation/Two Ray Ground
Antenna model	Antenna/Omni Antenna
Routing protocol	AODV
Simulation dimension	750 X 550
Initial energy in Joules	1000
Simulation time	150 seconds
Traffic	TCP
Channel type	Channel/Wireless Channel

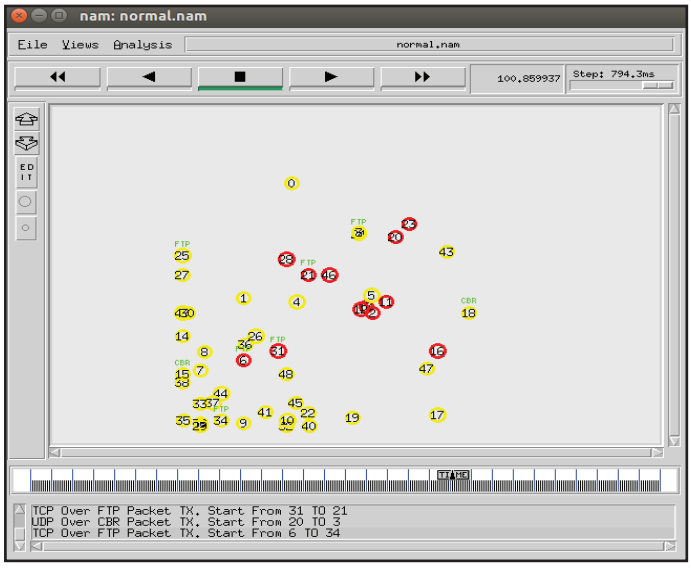

Fig. 1: Nam File of the Network Simulation

To calculate the better wormhole detection we need to add some of the quality measures which analyse various factors for improved bandwidth utilization, power saving & strong connections. For these performance evaluations, metrics includes following parameters such as PDR (Packet Delivery Ratio), Throughput and Routing overhead.

- **Normalized Protocol Overhead/ Routing Load:** Routing Load is the ratio of total number of the routing packets to the total number of received data packets at destination.
- **Packet Delivery Ratio (PDR):** Also known as the ratio of the data packets delivered to the destinations to those generated by the CBR sources. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol.
- **Throughput:** Throughput is the ratio of total number of delivered or received data packets to the total duration of simulation time.

In future the results will show the effectiveness of proposed scheme. For network simulation, there are several performance metrics which is used to evaluate the performance. In future simulation purpose this work will use different performance metrics for showing the expected results. Results are plotted using Xgraph utility of NS2

Fig. 2: Comparative PDR Graph for Normal and Proposed New

Graph Summary: As the PDR ratio is used to identify the performance of the approaches using the packet delivery ratio. It is the ration of number of packet sent to the number of packet received. In ideal condition it should be high as possible. For comparing the suggested work, the above graph interprets the result as an improved PDR ration than the existing approaches.

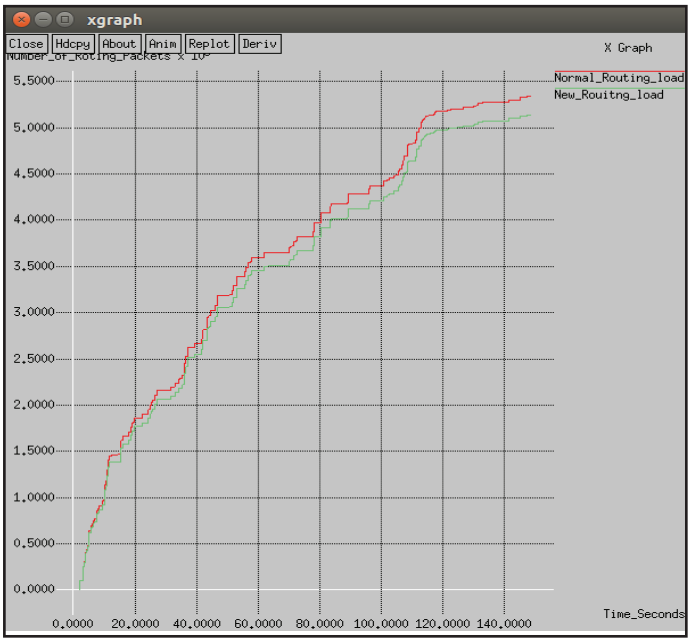

Fig. 3: Comparative Routing Load Graph for Normal and Proposed New

Graph Summary: The above graph verifies its results by minimum routing overhead associated with the suggested approach. It also shows that the complexity of using the proposed method is quite less in comparison with the existing.

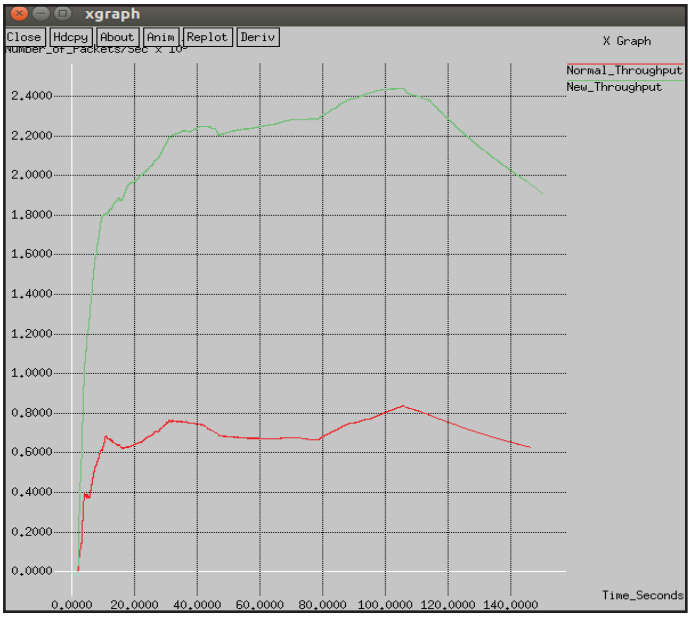

Fig. 4: Comparative Throughput Graph for Normal and Proposed New

Graph Summary: As throughput measure the transmission efficiency in terms of successfully delivered packets in unit time for a specified channel bandwidth. The above graph shows the effectiveness of the suggested approach while comparing it with the existing. The graph interprets the constant throughput for several cases which justify the approach.

A. Benefits of Approach

The suggested hybrid approach will serve as a improvement over the exiting attack and authenticity detection mechanism. The approach is a refined combination of different methods having capable functionalities for early and successful detection of malicious behaviour. The aim of approach is to identify the node giving consistent performance over the data transmission and taking this as a pattern and let the transmission of other node compare with it. After applying the above suggested approach there are some of the expected benefits measures are:

1. It provides security against modification, fabrication, replay, and impersonation attacks on MANET.
2. It gives low security overhead which considerably extends the network lifetime
3. It reduces the route setup delay and communication overheads.
4. It is cooperative for accomplishing high-level security with the aid of mutual collaboration/cooperation amidst nodes along with other protocols.
5. Public Key Cryptosystem will assure tight security in an light weight version of protocol.
6. Can be used for Multicasting or Unicasting scenarios
7. It is flexible enough to trade security for energy consumption.
8. It is compatible with the security methodologies and services in existence.
9. It is scalable to the rapidly growing network size.

B. Application

1. Video Conferencing
2. Multimedia Data Sharing
3. High Speed Video Network
4. VoIP Network
5. Secure Transmission with Complete Integrity Controls

IX. Conclusion

This paper proposes a novel hybrid mechanism for improving the security of MANET. Mainly the security here deals with the authentication and confidentiality of the data packets. The packets information here is encoded after separating them into categories or mutable information contains in them. Authentication is performed using digital signature algorithm SHA-I. Normally the approach verifies the non-mutable information with the unique signature associated with the packet. Encryption is performed with the RSA based public key cryptosystem. Thus the approach authenticates a sender and all the intermediate nodes in a multicast environment of mobile ad hoc network with a low computation overhead. The protocol assumes each node has pre-distributed secret key. In near future of implementation, extensive evaluation and experimental study will prove the results effectiveness of the suggested approach.

X. Future Work

While working on the above suggested phenomenon's it is found that some of the works are has to be taken relatively to solve the problems of wormhole detection. Also the performance evaluation is incomplete which can be verified completely after clear and effective implementation of the suggested work. In future some more comparison along with additional results can be taken for further verifying the approach authenticity. Some problems and concepts that remain unaddressed can be performed in future as a theoretical background, but the first thing is to develop a prototype so as to prove the results. It can also be used for quantitative & qualitative analysis etc. In order to detect outsider attacks or insiders malicious activity by personating the authenticity information, the proposed technique use larger number of control packet in future we will try negotiates that effect. For the future work, it may

be worthwhile to merge other solution improvement methods to improve the performance of the proposed approach, so that we can get good results when the number of mobile nodes is large and also the number of attacker nodes is much more.

References

[1] Sanket Nesargi, Ravi Prakash,"MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network", IEEE Transaction, 2002.

[2] Majid Taghiloo, Jamshid Taghiloo, Mehdi Dehghan,"A Survey of Secure Address Auto-Configuration in MANET", IEEE Transaction, 2006.

[3] El Hajjar, A.Lasebae, D.K.Saini,"Secure routing protocol for Mobile Ad Hoc Network using IPsec", Middlesex University, London, United Kingdom.

[4] Jared Cordasco, Susanne Wetzel,"Cryptographic vs. Trust-based Methods for MANET Routing Security", Department of Computer Science Stevens Institute of Technology, Hoboken, STM, 2007

[5] Manel Guerrero Zapata,"Middlesex University, London, United Kingdom", In Mobile Computing and Communications Review, Vol. 6, No. 3.

[6] Majid Tajamolian, Majid Taghiloo, Mahnaz Tajamolian, "Lightweight Secure IP Address Auto-Configuration Based On VASM", International Conference on Advanced Information Networking and Applications Workshops, IEEE Computer Society, 2009.

[7] Karamjeet Singh, Chakshu Goel,"Using MD5 AND RSA Algorithm Improve Security in MANETs Systems", In International Journal of Advances in Science and Technology (IJAST), Vol 2, Issue 2, June 2014.

[8] Khushdeep Kaur, Seema,"Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices", In International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 5, Oct 2012.

[9] Ramya K, Beaulah David, Shaheen H,"Hybrid Cryptography Algorithms for Enhanced Adaptive Acknowledgment Secure in MANET", In IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 16, Issue 1, Feb 2014.

[10] Lohar Priyanka D, Lomte Archana C,"UNIACK- Universal Adaptive Acknowledge Intrusion Detection System in Manets", In International Journal of Computer Applications (IJCA), Vol. 123, No. 4, August 2015.

[11] Aasia Samreen, Syed Irfan Hyderv,"Role of Threshold Cryptography in Securing MANETs", In IJCSNS, Vol. 15, No. 1, January 2015.

[12] Elhadi M. Shakshuki, Nan Kang, Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", in IEEE Transaction on Industrial Electronics, Vol. 60, No. 3, March 2013.

[13] Emmanouil A. Panaousis, George Drew, Grant P. Millar, Tipu A. Ramrekha, Christos Politis,"A Test Bed Implementation for Securing OLSR in Mobile Ad-Hoc Network", International Journal of Network Security & Its Applications (IJNSA), Vol. 2, No. 4, 2010.

[14] Harish Shakywar, Sanjeev Sharma, Santoh Sahu, "Securing OLSR and STAR Routing Protocols", International Journal of Computer Applications, Vol. 35, No.3, December 2011.

[15] D.Devi Aruna, Dr. P.Subashini,"Analysis of Different Propagation Model for IPSec-LANMAR Routing Protocol to Secure Network Layer for MANET in Emergency Area Environment", IJCST, Vol. 2, Issue 4, Oct. - Dec. 2011.

[16] Anil Suryavanshi, Dr. Poonam Sinha,"Efficient Techniques for SAODV in Mobile Ad-Hoc Network", Journal of Global Research in Computer Science, Vol. 2, No. 8, 2011.

[17] D.Devi Aruna, Dr.P.Subashini,"SNAuth-SPMAODV with IPSec to secure network layer for Mobile adhoc networks in Military Scenario", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 5, July - 2012.

[18] Prasad Chaudhari, Ms. Deepali Gothawal,"AuthMAN: Authentication in Mul ticast Mobile AdHoc Networks using Time Asymmetry", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (4), 2014.

[19] Jagrati Nagdiya, Shweta Yadav,"Secure Autoconfiguration in Mobile Ad hoc Networks using Rabin cryptosystem", IJETAE, Vol. 4, Issue 4, 2014.

[20] Venkateswara Rao Pallipamu, Thammi Reddy K, Suresh Verma P, "Design of RSA Digital Signature Scheme Using a Novel Cryptographic Hash Algorithm", In IJETAE, Vol 4. Issue 6, June 2014.

[21] Shelbala Solanki, Anand Gadwal,"Hybrid Security Using Digital Signature & RSA Encryption for AODV in MANET", in (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3), 2015.