International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.3, No.7, July 2014 DOI:10.15693/ijaist/2014.v3i7.144-153

IMPROVE DATA ACURRACY OF PACKET USING ADAPTIVE KEY SHUFFLING IN WIRELESS AD HOC NETWORK

[1]FEBIN SHERON P S, [2]DR.A.RAJARAM

[1]Research Scholar, Department of ECE, Karpagam University.coimbatore-641021

[2]Associate Professor, Department of ECE, Karpagam College of engineering, coimbatore-641032

Abstract: In Wireless ad hoc nodes are called as mobile nodes, these nodes are not place in constant position they are moved in any direction, packet drop is not fully detected from starting point to ending point by using normal detection technique. Disrupting packet transmission by attacker node available in routing path, it causes maximum end to end delay, since retransmission takes place. So proposed Adaptive Key Shuffling (AKS) method analyze the node generate packet size. It adds the key to packet, if any unwanted users try to capture the data, which are detected by this method. Attacker node is an unwanted user is named as data modification attack, it need to modify data's in packet, but key shuffling protect the data modification from particular node. Keys are shuffled in every packet, so third party node in network should not need to hack the data broadcasting. Key shuffling provides keys based on threshold range of packet size. It increases the packet delivery rate is a data accuracy, and detection efficiency, also reduce end to end delay.

Keywords: Adaptive key shuffling, data Accuracy of packet, rejecting intruder node

I.INTRODUCTION

Wireless ad hoc Network is the network that starts to perform packet transmission among source node to target node is credible missing any link connection. The wireless network is superior to wireless network since it minimized the resource utilization of additional connection is established to demanding host in the network environment. Then various nodes in wireless network are performing their position resourcefully to maintain the reliable link among sender to target node. Ad hoc network every nodes operate as sender and receiver side by side in network infrastructure [1].

There is no central ability node is present in this network for management of efficient packet sharing, whether the not use sink node to share data packets with any other nodes. The nodes in networks are normally separated into two kinds they are environment depending Network and No environment depending network. Environment wireless networks, wireless nodes should update its position when packet transmission made and sink nodes are placed, sometimes nodes move out of range from particular network that obtains different sink node in network environment [2]. When no Infrastructure less network is known as the ad hoc wireless networks, when packet transmission performed but no sink node and all nodes in network environment operates as senders and then this creates energetically network create packet transmission. The dissimilarity in Wireless Ad hoc network is obviously denoted in network [3]. The sensor networks are also measured as constant and updatable [4].

The sink node organizes the data packets from wireless nodes. It includes below the group of wireless node depends on network environment in updatable position of nodes with available sink node organize data packets with probable to nodes are transmit data packets with other lacking any availability of sink node and management environment. Except nodes connection contain more mistake proneness with less environments [5]. The intruder nodes are without difficulty degrades the network operations. Environment depending wireless sensor network are indicated, anywhere the source node need to share packets with target node else sink node among neighbor nodes and all network nodes are transmitted the combined data packets to sink node S [6].

The intruder node is forever the relay node and those nodes are initially affecting the network environment except those nodes first measure the packet data transmission and accurately operate such the normal nodes. Whether the source node starts to broadcast the data packets with instant intruder is operated, it need to loss data or damage the packets for transmission period [7]. A quantity of misbehaving nodes is also losses unnecessary data's in more quantity. The misbehaving nodes or intruder nodes are of different kinds such as black hole intruder, and wormhole intruders. The main goal of this type of intruders is to loss the useful data packet of source node and disgrace network communication. The general thing is wireless intruders is they each nodes are broadcasted wrong data packet [8].

Intermediate node is intruder that performs packet transmission to target node among wrong acknowledgement of original path packets. The wormhole intruder is similar to provide link and at the moment of packet delivery each information's are loss by intruder node. Intruder nodes are ready to create wrong acknowledgement packet in the network environment. The intruder is divided into various sectors and these sectors are mentions the intruder kinds in network environment [9]. The intruder plan is simply to loss the data, use network resource ability among the wireless nodes and transmit data packets with wrong individuality in network environment. For this study the various intruders are separated in wireless network and that kind of communication scheme is used for various paths [10].

Residual of the paper is designed as follows. Section II provides a related works. In section III, we present the details of proposed Adaptive Key Shuffling (AKS) method obtains a secured communication between wireless nodes, the best routing path is presented. Section IV provides simulation performance results analysis obtained under various metrics. At last section V concludes the paper with future direction.

II.RELATED WORKS

Patle, Amit, et al., [11] proposed the centre of reflection is on the protection problems connected to wireless sensor network routing schemes. Communication in WSN remainder an input problem since that lacking truthfully performance of communication conditions, the network plainly should not operate in the method. Unfortunately, communication must one of the most not easy to secure over intrusion caused by malicious behavior since of the direction in wireless sensor network. The efficient secure method is obtains the absolute protection from intrusions with the protection communication is obtains the effective and secure network process.

Chelani, Pooja L., et al., [12] present main need for the organization of packet transmission between various nodes in mobile network, which must work together with remaining nodes. Whether the malicious nodes are available, this needs make lead to severe protection worry such disturbing communication, packet latency and packet loss. It attempt to decide this problem by constructing an ad hoc distance vector routing based routing scheme that is considered to as enhanced bait identification method which combine merits of both practical and automatic defence system. Experimental output is provided presentation difference among the two nodes, node without applies enhanced bait identification method. Present is better transmission rate, lesser communication traffic with minimum energy usage compared to previous scheme.

Xin, Yonghui, et al, [13] present an Intrusion identification method depends on increasing entropy by analyzing the satisfied request irregular allocation and then obtain the misbehaving prefix classification scheme by relative entropy method. The importance trace back countermeasure is also used to hold back the intruder after identification. Consequently, the present method should minimize the wrong analyzing and security the justifiable node, and at the similar period, it keeps away from against response to normal traffic variation. Experimental solutions disclose that scheme can efficiently moderate in the Network.

Zheng, Yang, et al., [14] present suppose which started communication with a particular choice, in CSS equipment and less than the unbreakable result, this enhancement depending on the conventional energy consumption analyzing scheme which decide the entrance value by altering the connected metrics and apply the Neyman-Pearson principle that successfully oppose the misbehaving primary node emulation intrusion scheme. The experimental output indicates that the regular presentation of the enhanced energy usage identification is efficient than the usual energy identification scheme in the available network.

Govindasamy, V., .et al., [15] present intense on recognize previous the misbehaviour characteristics in Mobile network environment. The answer by propose Adaptive Approach identification using Key allotment technique with Shuffling method. It minimizing the collision of key organization depend influence guarantee and created higher tolerance range without support the nodes in network. This manages the different intrusions counting also identify of black hole intrusion with lesser packet transmission charge in the MANET. A challenger can effectively fixes black hole intruder node in routing path, at last to confirm that using this method should improve the Mobile network protection that enhances the privacy and reliability.

Khan, Muhammad Saleem, et al., [16] present a novel ATT-Adaptive Trust Threshold estimation method, which adapt the secure threshold in the communication condition according to network rules like a rate of connection updates, node movement range with link availability, with average neighbourhood trustworthiness. To identify the topology factors those affect the secured entrance value at all nodes

and authority them to construct a calculation model for this calculation. Experimental output shows that the secured scheme obtains important increasing the packet delivery ratio, decrease in false positives, and enhance in attack identification ratio as distinguish with usual constant threshold scheme.

Pushpa, A. Menaka, et al., [17] proposed intelligent adversary introduces the intruding scheme on MAC layer over attack removal method only when it can increase high in an intrusion achievement ratio. Experimental survey it observes the strength of mobile ad hoc network over this interior intruder method. Multicast session presentation parameters like packet delivery ratio, transmission rate and packets loss rate are measured with the attendance of intruders in the multicast scheme. It examines the crash of intruder node position in the multicast routing path. To construct a systematic model that indicates the collision of internal intruder on multicast group among empirical survey. Experimental output should distinguish to confirm the strength of analytical design.

Al-Hujailan, Hajar, et al., [18] present protection over each network intrusion that is identified by any node in the infrastructure, for particular identifies the transmitter. It is easy, dependable, successful and its behavior not precious by position of path allocation. A new attacks identification method for grouped a mobile network that exceed the disadvantage and removes the boundary. Present method warns each node in the network beginning a attacker node give to be certain that the node is actually misbehaving. The network nodes collaborate to obtain clear of the attack possessions. To minimized the false encouraging rate decreasing in the traffic rate.

Ghosh, Uttam, et al., [19] proposed a novel signature method that confirm and reduce the protection problems connected with dynamic IP arrangement. Confirmation of rightness of the present mark method verifies which method is protection over any fake intrusion. Extensive Experimental output indicates that the present indicating method has lesser traffic rate and minimum delay for packet transmission with additional Protection method is distinguish with previous updatable arrangement techniques. Furthermore, it is strong also better to answer the issues of network separation and combining.

Tiwari, Prachi, et al., [20] present awareness and arrangement of Wireless Ad hoc network generates them smooth to be easily intruded using frequent methods often used beside wired networks as well as recent scheme particularly to network. Protection problems starts in many various field including with objective protection, key organization, communication and attack identification with removal are important to a useful updatable network environment. It mainly indicates the security problems. Communication maintains a key concern since lacking of truthfully process of routing conditions, the network will not work powerfully, regrettably, routing is also most difficult to protect next to intrusion of misbehaviour node are removed. It secures packet transmission between wireless ad hoc nodes in network environment.

III.OVERVIEW OF PROPOSED SCHEME

In Wireless ad hoc network is a movable network; nodes are freely updating its position along the environment. The each position of node is noted in routing table, since packet loss occurred for every time because of attacker node present in network. It detects and remove the attacker nodes that data modification in WANET. Proposed key shuffling operates successfully by chance selection of the neighbouring nodes.

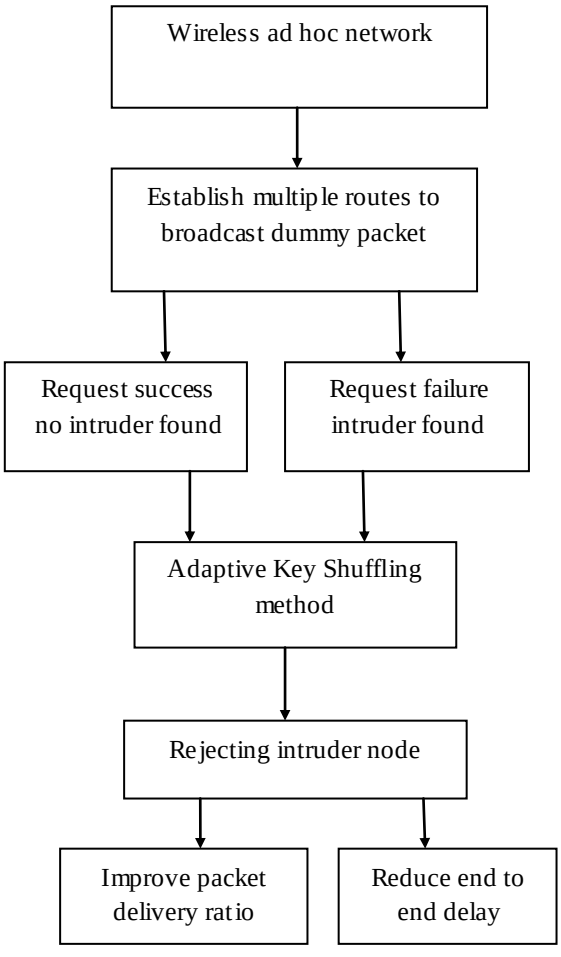

Figure 1: Block Diagram of Adaptive Key Shuffling method

Figure 1 shows Adaptive Key Shuffling method provides secured communication. It establishes the multiple routes to broadcast dummy packets. Request successfully transmitted there is no intruder node found otherwise intruder node found. Adaptive key shuffling method shuffles the keys in data packets every time. And then detect and reject the intruder nodes from network, it improves packet delivery rate and minimize end to end delay.

Keys are attached to the packets; size of packet is varied so interchange the keys for every packet, intruder node not captures data's. The key are changed in very packet transmission, attacker could not knows the original key, so attacker not affect the packet transmission, then attack detection efficiency is improved and end to end delay is reduced.

3.1 Establishing Multiple Routes broadcast dummy packets

Sender node need to broadcast data on multiple routes. The created route is random. It contains amount of nodes that are uninformed for source and destination node. Sender node wants to transmit dummy packet, it's like a hello packet to intermediate node in routing path. Intermediate node may answer by reply packet for particular time period. The sender node is dependable for selecting an efficient node that broadcast data packet to destination node. The sequence intermediate node should work as Sender Node and this communication is repeated until target node does not accept the packet or the packet terminate. Then achieve the source node secrecy all nodes is limited then not use individual hop intermediate nodes that is it not easy to analyze the network environment then consider current node is sender node which broadcast packets.

A path finding process in ad hoc network uses request and reply packets which are maintained in routing table. Path building process initiates with originate request message packet by the sender node that needs to add the multicast packet transmission. Whether the node previously know sender and target node which has a route for packet transmission, then the node only transmit single request packet to target node through intermediate relay nodes. Otherwise whether the node does not have various paths to the target node, it transmits a request packet message. This request packet either broadcast in sequence to discover a route for recently adding node in the multicast network. Nodes of the multicast network should only provide acknowledgement for request packet by broadcasting reply message. Reply packet transmits towards the sender node of request through reverse way. Reverse indicator is recognized, while the request message is broadcasting by destination node through the routing path, where $B(Dpack)$ dummy packet is broadcasted.

$$M_R = B(Dpack) - (1)$$

Whether there are no previous multi request transmission nodes in the network, request packet is transmitted additional awaiting it reach the destination node. Request packet is reply by also target node or any multi process performer node in the network. A sender node may be accepts many reply packets from various nodes in the multicast network. Broadcaster indicators contain the path when reply packet movements reverse to the sender of request packets. Sender node chooses the path among that provides the connection to target node, then nodes perform multiple tasks. Sender node sends the authentication message to the chosen intermediate nodes in network until it reaches the sender node of the reply packet. Request packet, reply packet, also path finding control message are transmitted in order to provide path through the multicast intermediate nodes. Where $Dreq$ dummy request is estimated as:

$$B(Dpack) = B(Dreq) - (2)$$

$$B(Dreq) = Nb + nNb - (3)$$

The single cast scheme is broken by the intruder node for its intrusion approach. Normal attack prevention method and intrusion approach of internal quiet intrusion. In path finding procedure uses a single cast method, while multicast packet overload utilize individual nodes packet transmission techniques. The path finding process is troubled by processing intrusion approach over combined method. Intrusion causes over an MAC layer accident removing method available by network. Intruder not use the CA method instruct by medium access control layer, while it single cast path finding packets. Intruder rejects the handshake method earlier than it broadcast control message, like request, reply and Control packets. Next time slots, the intruder broadcasts control message to its destination node.

3.2 Adaptive Key Shuffling for data packets

Data packets are loosed at intermediate relay node owed to demanding condition. Reply packet is loosed at accepter node. The sender re broadcast the similar reply packet at Maximum

range. Repeat calculation, whether it fail for the higher repeat calculation, then losses the data's at MAC source node. Subsequent MAODV control packets are losses by this intruder reply packet, Path Request single cast, Path reply, collection dummy packets and current position of intruders in the routing path that acting an important function in this intrusion. The intruders achievement rate is very high only in the subsequent rules are Many paths are used to transmit data packets through any intrusion or distrustful node. Then nNb next neighbor node of multi task performer by sender as well as the sender node contain solitary route that links the sender node with previous path constructing schemes.

$$nNb = MT(s) - (4)$$

Interior distrustful node works a misbehaving over collision prevention method only while it can increase more in aggressive success rate in the multi task performer nodes, therefore, while a distrustful node recognize the survival of multicast sender or accepter node in its communication area, then this current node should initiate to activate intrusions on the network. In that way, interior node brightly implements intrusion only, while it can have higher attacking success rate. As an alternative of executing attacks at arbitrary time slot, this scheme provides a high success rate with minimum possibility to discover by attack identification scheme in the multi task performer. In addition the location of the intruders in multitask path is important for attack identification.

$$MT(s) = \iint \log s * \log s - (5)$$

Malicious nodes should loss packets for every transmission change or insert wrong data to packets. Proposed method key shuffling is implemented so, adaptive keys are inserted and attack identification and misbehaving node separation method is implemented at all node and is able of identifying malicious from remaining other nodes. The attack identification method should activate the adaptive trust entrance scheme unit when an attack is identified. Then it is important to indicate that, the reliability of all intermediate nodes are state limited to all node, all node need to execute process separately. This technique is used for adaptive security estimation is entirely dispersed, and consequently various nodes strength contains various vision of the similar intermediate nodes, this scheme separating the intruder nodes from routing path in network with also to point out optional path available in network environment.

$$MT(s) = 2\iint \log s - (6)$$

$$nNb = 2\iint \log s - (7)$$

Keys are added to packet before transmission, every time key is shuffled because the third user cloud not knows the shuffled key inserted in data packets. It is adaptive key so securely broadcasted from source node to target node in network environment. That information is not hacked by intruder but it tries much time to block the original data for packet transmission. Destination gives reply packet while packets are successfully received. Reply packets broadcasted in reverse direction.

Algorithm for Adaptive key shuffling

Step1: Analyze node position.

Step 2: For each sender node sense intermediate nodes

Step3: Adaptive key added to packet

Step 4: Implement key shuffling in every time for packet transmission
Step 5: if {intruder==available}

Step 6: Try to hack the original packet but key shuffling improves the performance

Step 7: else

Step 8: if {intruder==not available}

Step 9: continue packet transmission in same routing path

Step 10: Initially dummy packet are forwarded

Step 11: After get acceptance original data packets are broadcasted

Step 12: end if

Step 13: end for

3.3 Rejecting intruder node with support of Adaptive key shuffling

The node quantity contains a straight collision on the security limits. When estimating the entrance, all nodes contain the node quantity in its single hop intermediate nodes. The maximum the amount of nodes in its single hop intermediate nodes, the high level the threshold limit. In truth, while a sender node has more option single hop

relay nodes for choosing as broadcasting nodes, it can stand stricter threshold limits with minimum possibility for network separating. Whether a misbehaving node is inaccessible from the communication route, node remainder linked to the network with it has much optional broadcasting nodes, guarantee a steadiness among high path discovery rate and packet transmission rate.

$$B(Dreq) = Nb + 2\iint \log s - (8)$$

$$Nb = \iint \log s - (9)$$

The node link establishment is another vital restriction for Adaptive key shuffling scheme, indicating the acceptance of the network to node failure. Its reason is to make sure the link of network before separating a malicious node from the communication route. Then it identifies the best entrance charge at node for the probable rejection of intruder node in routing path. The work of the network with the next neighbor of all node transmission takes resource utilization regularly for network's speed. A node should decide its intermediate node speed by computing the relay node rate of connection updates. A Maximum speed makes to an advanced rate of connection updates in network.

$$B(Dreq) = \iint \log s + 2\iint \log s - (10)$$

$$M_R = 3\iint \log s \text{ - } (11)$$

For security depending methods, all node handle a secured routing table to evidence the security of other remaining nodes, consequently the average intermediate relay nodes dependability is easily estimated. The entry of particular table for all intermediate nodes in this scheme, are estimated by analyzing the proportion of packets accurately Broadcasted by that relay nodes in a descending most recent simulation characteristics. Present method, obtains higher packet delivery rate and minimum packet latency.

Algorithm for Rejecting intruder node with support of AKS

Step 1: Link between nodes is established.

Step 2: for each search intruder node from routing path.

Step 3: if {low trust==unsecure}

Step 4: identify intruder node

Step 5: reject that node from entire network environment

Step 6: else

Step 7: if {high trust==secure}.

Step 8: use that node to broadcast packet use AKS

Step 9: End if.

Step 10: End for

This scheme improves the security so all packet are delivered successfully from source node to destination node. There is no need to rebroadcast the data packets so packet latency is minimized, intruder nodes are earlier to detect and reject from routing path in network.

Packet ID: Packet ID has all wireless ad hoc node information. It also obtains the current position of node to support for path construction in network environment.

Source ID	Destination ID	Multiple Routes broadcast dummy packets	Adaptive Key Shuffling for data packets	Rejecting intruder node	Improving packet delivery ratio
3	3	5	5	5	4

Figure 2: Proposed AKS Packet format

In figure 2: the proposed AKS packet format is shown. Here the source and destination node ID field takes 3 bytes. Third one is Multiple Routes broadcast dummy packets contains 5 bytes. Initially sender check the neighbor node it is intruder or true node use dummy request packet. In fourth field occupies 5 bytes. Adaptive Key Shuffling for data packets, it improves packet delivery ratio keys are generated and added to packets before start packet transmission and they are mixed in every time. In fifth occupies 5 bytes, rejecting intruder node from entire network, remove the intruder node based on node behavior in network. The Improving packet delivery ratio, it occupies 4 bytes, to choose only best node use key shuffling increase transmission rate in routing path.

VI. PERFORMANCE EVALUATION

A. Simulation Model and Parameters

The proposed AKS is simulated with Network Simulator tool (NS 2.34). In our simulation, 100 wireless ad hoc nodes are placed in a 1000 meter x 1000 meter square region for 30 milliseconds simulation time. Each Mobile node goes random manner among the network in different speed. All nodes have the same transmission range of 250 meters. CBR Constant Bit Rate provides a constant speed of packet transmission in network to limit the traffic rate. DSDV Destination sequence distance vector routing protocol is used to assign best routing path for packet transmission. Table 1 shows Simulation setup is Estimation.

Table 1: Simulation Setup

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11g
Radio Range	250m
Simulation Time	16ms
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	DSDV

Simulation Result: Figure 3 show that the proposed AKS method provides secured routing with high packet delivery ratio is better compared with existing ATTS [16] and ADS [20]. AKS has adaptive key they are get shuffled in every time, key is inserted into packet to make efficient communication also detect and remove if any intruder node present in network environment. It improves the packet delivery ratio and minimizes end to end delay in network.

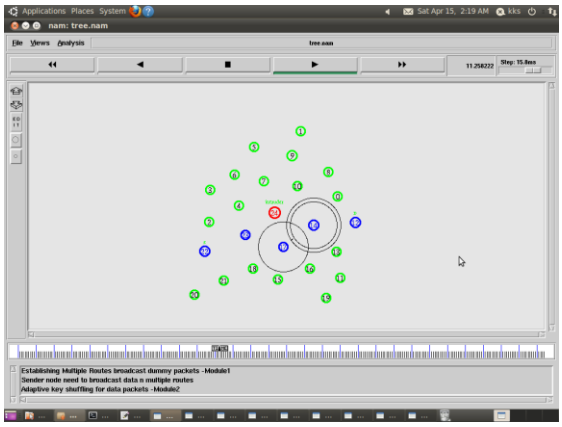

Figure 3: Proposed AKS Result

Performance Analysis

In simulation to analyzing the following performance metrics using X graph in ns2.34.

End to End Delay: Figure 4 shows end to end delay is estimated by amount of time used for packet transmission from source node to destination node, key shuffling scheme protect the packet transmission. In proposed AKS method end to end delay is reduced compared to Existing method ATTS and ADS.

$$End\ to\ End\ Delay = End\ Time - Start\ Time$$

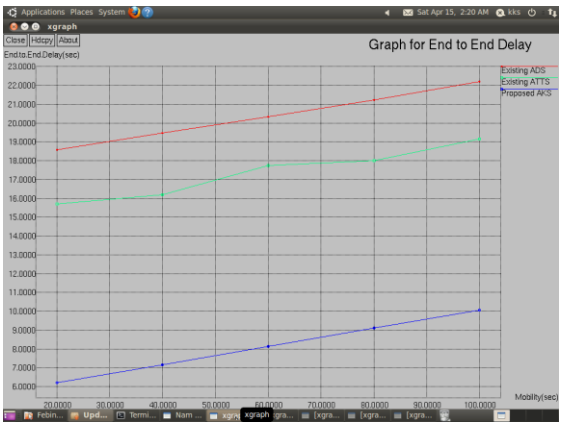

Figure 4: Graph for Mobility vs. End to End Delay

Communication overhead: Figure 5 shows communication overhead is minimized in which sender transmit packet to receiver node, adaptive key shuffling not allows retransmission of packet, it provide data packet transmission with high security. In proposed AKS method Network overhead is minimized compared to Existing method ATTS and ADS.

$$Communication\ overhead = (Number\ of\ Packet\ Losses/Received) * 100$$

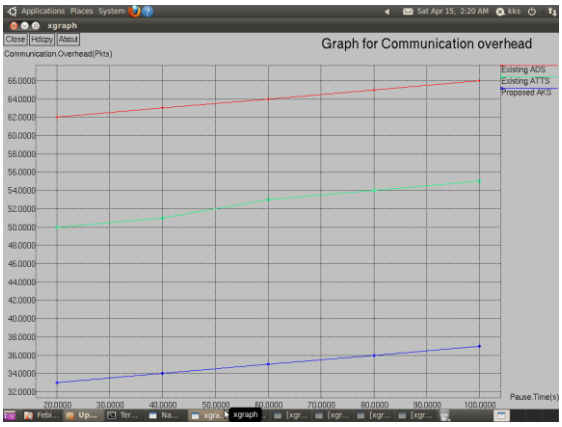

Figure 5: Graph for Pause time vs. Communication overhead

Packet Delivery Ratio: Figure 6 shows Packet delivery ratio is measured by no of received from no of packet sent in particular speed. Node velocity is not a constant, simulation mobility is fixed at 100(bps). In proposed AKS method Packet delivery ratio is improved compared to existing method ATTS and ADS.

$$\textit{Packet Delivery Ratio} = (\textit{Number of packet received/Sent}) * \textit{speed}$$

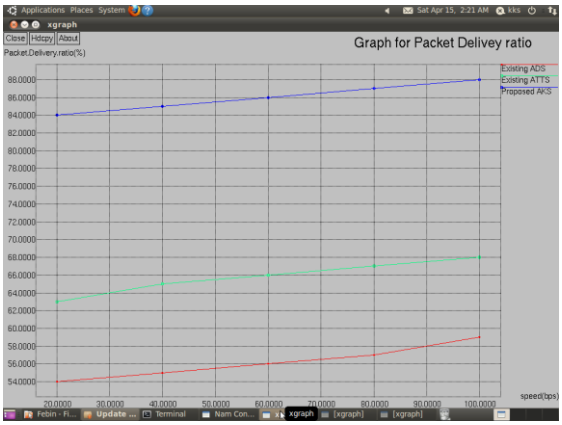

Figure 6: Graph for Nodes vs. Packet Delivery ratio

Detection efficiency: Figure 7 shows Detection efficiency, attacks are occurred packet transmission is repeated from source node to Destination node. Time spent to detect the intruders. In proposed AKS method detection efficiency is improved compared to Existing method ATTS and ADS.

$$\textit{Detection efficiency} = \textit{attack detection rate/overall time}$$

Figure 7: Graph for Nodes vs. Detection efficiency

Network Lifetime: Figure 8 show that Lifetime of the network is measured by nodes process time taken to utilize network from overall network ability, it use key shuffling to mixing the keys in data packets. In proposed AKS method network Lifetime is increased compared to existing method ATTS and ADS.

$$\textit{Network Lifetime} = \textit{time taken to utilize network/overall ability}$$

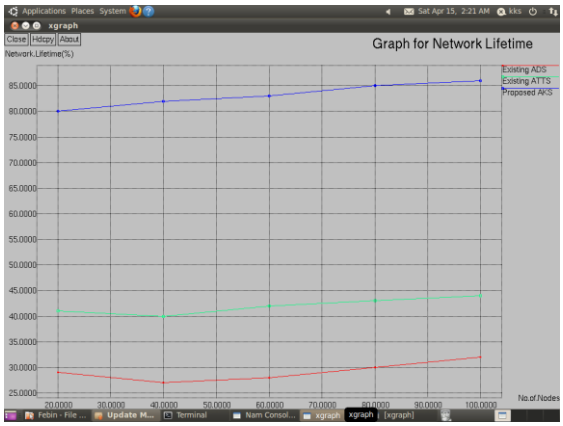

Figure 8: Graph for Nodes vs. Network Lifetime

Packet Integrity rate: Figure 9 shows that Packet integrity of particular communication in network is estimated by nodes transmit packet with key and without key those keys are shuffled. In proposed AKS method Packet Integrity rate is improved compared to existing method ATTS and ADS.

$$Packet\ integrity\ rate = \left(Number\ of\ packet \frac{Successfully\ sent\ with\ key}{Successfully\ sent\ without\ key}\right) * 100$$

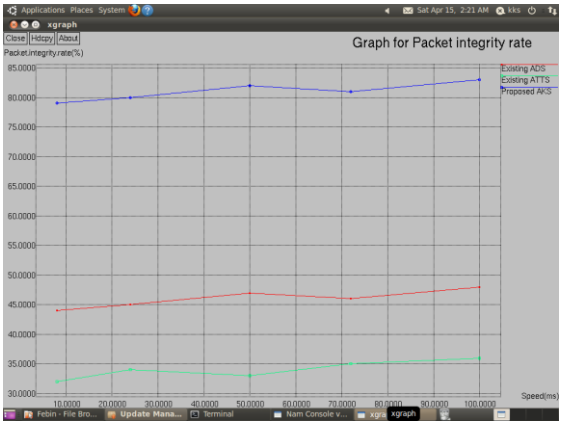

Figure 9: Graph for Speed vs. Packet Integrity rate

V. CONCLUSION

In wireless ad hoc network contains a wireless nodes like mobile nodes that perform packet transmission but intrusion made they need retransmission at every time, so packet latency occurred, also node could not receive packets successfully. Proposed AKS method to provide adaptive key they are inserted into every packets before that are transmitted. Establishing the multiple routing path for broadcast dummy request packets to destination node, if it true nodes packets are received otherwise intruder nodes packets are not received, so there is no reply packet send to source node in reverse direction, keys are shuffled in packet so intruders not easy to hack efficient communication. It detect and reject intruder nodes which present in routing path, it improves packet delivery ratio and minimize end to end delay. In future presents modified adaptive key shuffling to measure different parameters in wireless network.

REFERENCES:

[1] C Siva Rama Murthy C. and B.S Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Second Edition, Low price Edition, Pearson Education, 2007.

[2] Junbeom Hur and Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", Member, IEEE, ACM, IEEE/ACM Transactions on Networking, Vol. 22, No.1, February 2014.

[3] Y. Khamayesh, R.Salah, M.B. Yassein, "Malicious Nodes Detection in MANETs: Behavioral Analysis Approach", Journal of Networks, Vol.7, No.1, January 2012.

[4] K. Fall, "A Delay Tolerant Network Architecture for Challenged Internets," in Proceedings of SIGCOMM '03, pp. 27-34, 2003.

[5] Luming Wan, Feiyang Liu, Yawen Chen, and Haibo Zhang, " Routing Protocols for Delay Tolerant Networks: Survey and Performance Evaluation", International Journal of Wireless & Mobile Networks (TJWMN) Vol. 7, No.3, June 2015.

[6] T. Burgess, G. Bissias, M. Corner, and B. Levine. Surviving attacks on disruption-tolerant networks without authentication. In Proceeding of ACM MobiHoc, 2007.

[7] Rakhi Sharma and Dr D.V Gupta, "Blackhole Detection and Prevention Strategies in DTN", International Journal Of Engineering and Computer Science, Volume 5 Issues 8, pp. 17386-17391, August 2016.

[8] Chlamtac, I, Conti, M, and Liu, J. J. N. Mobile Ad hoc Networking: Imperatives and Challenges", Ad Hoc Networks, 1(1), pp. 13-64, 2003.

[9] Mohit Kumar and Rashmi Mishra, "An Overview of MANET: History, Challenges and Applications", Indian Journal of Computer Science and Engineering (lJCSE), Vol. 3 No. 1 FebMar 2012.

[10] Mengjuan Liu, Yan Yang, Zhiguang Qin, "A Survey of Routing Protocols and Simulations in Delay-Tolerant Networks", Chapter of Wireless Algorithms, Systems, and Applications Volume 6843 of the series Lecture Notes in Computer Science, 6th International Conference, W ASA 2011, Chengdu, China, pp 243-25, Springer, August 11-13, 2011.

[11] Patle, Amit, and Neetesh Gupta. "Vulnerabilities, attack effect and different security scheme in WSN: A survey." ICT in Business Industry & Government (ICTBIG), International Conference on. IEEE, 2016.

[12] Chelani, Pooja L., and Sudhir T. Bagde. "Detecting collaborative attacks by malicious nodes in MANET: An improved bait detection scheme." Communication and Electronics Systems (ICCES), International Conference on. IEEE, 2016.

[13] Xin, Yonghui, et al. "A Novel Interest Flooding Attacks Detection and Countermeasure Scheme in NDN." Global Communications Conference (GLOBECOM), 2016 IEEE. IEEE, 2016..

[14] Zheng, Yang, et al. "A scheme against primary user emulation attack based on improved energy detection." Information and

Automation (ICIA), 2016 IEEE International Conference on. IEEE, 2016.

[15] Govindasamy, V., S. Sandosh, and C. Suraj Kumar. "KD2SA: Key Distribution Scheme Shuffling algorithm for heightened secure data transmission." Computation of Power, Energy Information and Commuincation (ICCPEIC), 2016 International Conference on. IEEE, 2016.

[16] Khan, Muhammad Saleem, et al. "Adaptive trust threshold strategy for misbehaving node detection and isolation." Trustcom/BigDataSE/ISPA, 2015 IEEE. Vol. 1. IEEE, 2015.

[17] Pushpa, A. Menaka, and K. Kathiravan. "Intelligent stealthy attack on MAODV in mobile ad hoc networks." Advanced Computing (ICoAC), 2014 Sixth International Conference on. IEEE, 2014.

[18] Al-Hujailan, Hajar, Mznah Al-Rodhaan, and Abdullah Al-Dhelaan. "A cooperative intrusion detection scheme for clustered mobile ad hoc networks." Information Assurance and Security (IAS), 2011 7th International Conference on. IEEE, 2011.

[19] Ghosh, Uttam, and Raja Datta. "A novel signature scheme to secure distributed dynamic address configuration protocol in mobile ad hoc networks." Wireless Communications and Networking Conference (WCNC), 2012 IEEE. IEEE, 2012.

[20] Tiwari, Prachi, and S. Veenadhari. "Attacker and different security scheme in Delay Tolerant Wireless Ad hoc Network." ICT in Business Industry & Government (ICTBIG), International Conference on. IEEE, 2016.