ISSN: 2321-7782 (Online)
Volume 2, Issue 2, February 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Enhanced S-ACK with MRA and Level Analysis for MANETs

S. Raji[1]
M.E
Network Engineering
Francis Xavier Engineering College
Tirunelveli - India

Dr. R. Ravi[2]
M.E., Ph.D
Professor & Head of CSE
Francis Xavier Engineering College
Tirunelveli - India

Abstract: ***In contrast to traditional network architecture, Manet does not require a fixed network infrastructure; every single node can act as a transceiver. Manet nodes are capable of self- configuring mission critical applications such as emergency rescue and military use. When they are both well within the range of communication nodes communicate directly with each other. However, the open medium and wide distribution of nodes are vulnerable to malicious attacks. In this case, it is important to develop methods of intrusion detection effectively protect from attacks unchanged. Here, we improved the safe acknowledgment of the request and implement a new intrusion detection system. In order to make a more security to mobile network than existing system, we are proposing a new technique known as hashing technique i.e. node verification technique for intrusion detection system, in addition to that we are going to calculate the energy level for each node. This can be done by means of analysis of the level of confidence.***

Keywords: Mobile Ad hoc NETwork (MANET), DSR (Dynamic Source Routing), S-ACK (Secure ACKnowledgement).

I. INTRODUCTION

MANET places that can configure itself for a change and is a type of temporary network. Manet's nodes are mobile because they use wireless connections to connect different networks. Such as a cellular or satellite to a standard Wi-Fi connection. For example, a VANET (Vehicular Ad Hoc Networks) , that allows vehicles to communicate with roadside equipment is a type of Manet. Each device in a Manet is free to move freely in any direction, and therefore change its links to other devices frequently. Each forward traffic unrelated to its own use, and should therefore be a router. Manet continued right through the building of a primary challenge is to transport the necessary tools for each device to maintain the information. Such networks or the Internet connection will work themselves. This includes vehicle and tricks Networks (VANETs) are used to communicate between vehicles in the roadside equipment. Internet -based mobile ad hoc networks (iMANET), that connect the nodes and edges are fixed internet portals. It cannot apply directly to ordinary individuals, such as networks, routing algorithms. Intelligent Auto temporary networks (InVANETs) a lot of research in the past has been for example move the vehicle to vehicle collisions, accidents, drunken driving , while rational behavior vehicles that serves the artificial intelligence of a sort , but the most significant contributions are PGP (Pretty Good Privacy) and faith-based care , but anyone with a decent trading protocols between security and performance[4] . Many researchers in an effort to increase security protocols for MANETs and some new regulations to implement the advice and counsel of the new improvements. The attacks on MANETs routing nodes can join and easy to go on a fixed route requests to the dynamics of the mobile infrastructure, which can be challenging. Following are the attacks which are occur in layers of the OSI Model. Application layer: Malicious code, Transport Layer: Session traffic hijacking, flooding the network. Network layer : Sybil, floods , Black Hole , Worm Hole , link spoofing , unauthorized connection was made , Data link / MAC layer: malicious behavior , self-interested behavior , active attack , passive attack, internal and external attack ,Physical layer : interference , traffic collision . Proactive and Reactive are basically two approaches to protecting MANETs [9]. Proactive approach by the various encryption techniques, trying to prevent an attack from launching

attacks in the first place. In contrast, reactive approach to detect security threats and react accordingly like posterior. MANETs is a complete security solution to integrate approaches to include three elements: prevention, detection, and reaction. For example, when a packet functions can be used to protect by means of reactive approach, proactive approach can be used to ensure proper routing states. As argued in, security is a chain based, and it is only as protect as the simple weakest link.

Missing an each single component may significantly degrade the overall security solutions. The protocol can be classified into two types. The proactive protocols are extensions of the wired network routing protocols. They are maintaining the global such as common topology information in the form of tables at every node. This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. These tables are updated frequently in order to maintain consistent and accurate network state information. Routing information is generally flooded in the whole network, whenever a node requires a path to the destination node, it runs like an appropriate correct path finding algorithm on the topology information it already maintains. The Destination sequence Distance-vector routing protocol(DSDV), Source tree adaptive routing protocol(STAR), Wireless routing protocol(WRP) and Cluster head gateway routing protocol(CSGR) are some examples for the proactive routing protocol[3]. Unlike the Table driven routing protocols, Reactive routing protocols execute the path finding process and exchange routing information only when a path is required by a node to communicate with a destination. The protocol fall under this category do not maintain the network information. They obtain the required path when it is necessary, by using a connection establishment process. The Dynamic source routing protocol (DSR), Temporally Ordered Routing algorithm (TORA), Adhoc On-Demand Distance vector routing protocol etc. A good routing protocol for this network environment has to dynamically adapt to the changing network topology. This Hybrid type of protocol combines the advantages of proactive and reactive routing protocol functions. The routing is initially started with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. Nodes within a certain distance from the node concerned .or within a particular geographical region are said to be within this zone, a table driven protocol is used. For nodes which are located beyond that zone, an on-demand approach is used. The Zone Routing protocol (ZRP), Zone based Hierarchical Link State routing protocol (ZHLS). The main disadvantages of such algorithms are: Advantage depends on number of other nodes activated; Reaction to traffic demand depends on gradient of traffic volume [2]. The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network [5]. **Route Discovery** is the mechanism by which a node Swishing to send a packet to a destination node D Obtains a source path to D. Route Discovery mechanism is used only when S attempts to send a packet to D and does not already know a path to D. **Route Maintenance** is the mechanism by which node S is able to find, while using a source path to D, if the network topology has changed such that it can no longer use its path to D because a link along the path no longer works. When path Maintenance indicates a source route is broken, Source can attempt to use any other route it happens to know to Destination, or it can invoke Route finding mechanism again to search a new path. Route Maintenance is used only when Source is actually sending packets to Destination. DSR does not use any periodic routing advertisement, like link status sensing, or neighbor node detection and does not relies on these functions from any underlying protocols in the network.

II. PREVIOUS WORK

A. *Acknowledgement Scheme*

An end-to- end acknowledgment scheme based on nominal Acknowledgement. It aims to reduce the network load on the network and when misconduct is detected [1]. Nodes S and T between the way all intermediate nodes cooperative and node successfully transmits the packet Pad1, node D is receiving that packet. Now , the tip of the destination node D is a building to demolish the data packet Pad1 sends out the same way but in a reverse order of a building Pak1 to send an acknowledgment packet back down. If that Pak1 (Acknowledgement) is not received by the sender means it establishes the Secure Acknowledgement mode.

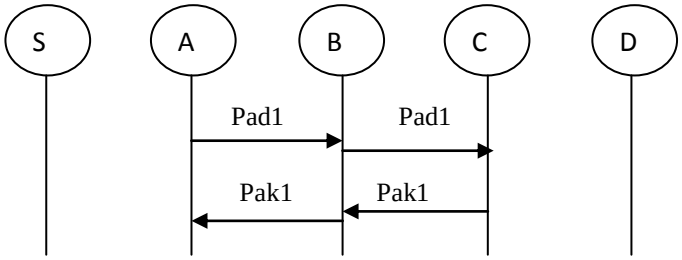

Fig 1: Acknowledgement Scheme

B. *Secure Acknowledgement Scheme*

S- Acknowledgement scheme is an improved version of the Acknowledgement program [1]. Each of the three nodes continues to work as a team to identify faulty nodes. In each of these three fronts, the third node to the first node to send an acknowledgment packet. S- Acknowledgement receiver with the intention of introducing the conflict or faulty nodes to detect even with the presence of limited transmission power.

C. *Misbehavior Report Authentication*

The plan is to escape the presence of misconduct could not be found on the wrong end of the weakness of the monitoring is designed to solve. Report misconduct can be created by a malicious attack by malicious nodes were innocent. For a network whose nodes are sufficient to cause the attackers to break down the entire network when the attack can be lethal. The main goal of the project is to escape through a different path to the node that contains the information of the missing packet, acknowledge it. He escapes from the start, from the source node and the destination node searches its local knowledge base and search for alternatives [6][7] .The source node is to find another route with a request of the DSR routing . Due to the nature of MANETs, it is common to find many ways between the two nodes. By adopting alternative target node, we pass the point of reporting misconduct. When the node receives a packet depends on its local knowledge base searches and compares the data packet is received. Otherwise, reliable and accepted the report of misconduct. Since the adoption of the escape plan, EAACK misconduct, despite the existence of the report is the ability to detect malicious nodes. As discussed before, EAACK is an acknowledgment - based IDS. EAACK in three areas, ie, Acknowledgement S-ACKAcknowledgement, Misbehavior Report Authentication, Will be executed based detection schemes. All of them depend on an acknowledgment packet network to detect misbehaviors . Therefore, it is important to make sure that is true all acknowledgment packets.

III. PROPOSED SCHEME

In order to provide more security to mobile adhoc network than existing system, we are proposing a new technique known as hashing technique i.e. node verification technique for intrusion detection system and calculating energy level for each node.

A. *Hash Technique*

The hashing technique is an generation of hash id to mobile nodes H(n) = public key/identity. If any node in the network wants to verify neighbour node or any other node , the particular node X request a neighbour node Y to generate a hash id using hash function. The Y node generates hash id using a public key of X and identity of Y. in the same X node also generates a hash id using public key of Y and identity of X. if both the hash id are equal then the nodes are authenticated and not a malicious node. If Y node hash id is not equal to X node hash id then the corresponding Y node is malicious node. Then the detected malicious node is eliminated from the network. In this way our proposed technique detects and eliminate malicious node. Any node can verify any other at any time, by this intrusion detection system all nodes in the network can be verified and we can form a securable network. Hashing techniques are available based on the concept of a hash function that it transforms a given input value of arbitrary length to a value of a stable length, called the hash value. The transformation is done in a manner, it is computationally infeasible to transform the hashing value to the true value. Hash functions are most efficient as they don't

involve heavy calculations and hence they are applied in the area of security for information authentication and value of integrity checks.

B. ***Energy Level***

In this system the intrusion detection system detects the malicious node by calculating energy level for each node. This can be done through trust level analysis algorithm. In this technique we are going to calculate the energy level for each node , generally the malicious nodes have three times more energy value compared to normal nodes. By analyzing the energy level of all nodes we can easily detect and eliminate the malicious nodes from network. For example maximum nodes will have energy level as 23 joules, the malicious nodes have more than 60 joules, by observing the values we can detect the malicious.

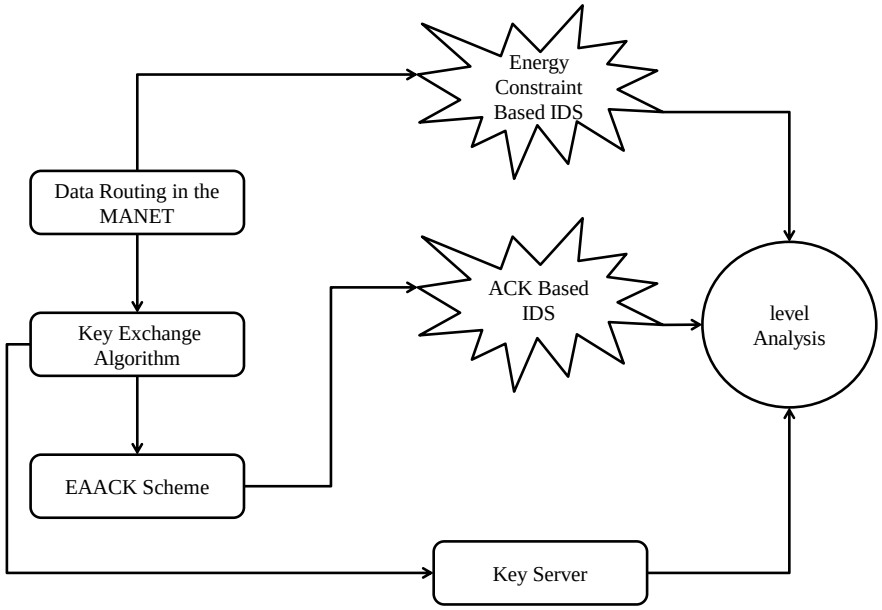

Fig 2: System Overview

C. *Modules Description*

1) *Home agent*:

The present in each network and it gathers information about its system from application layer to routing layer in OSI model.

2) *Neighboring node*:

Any system in the network transfer any type of information to other network system, it will broadcast through some intermediate nodes. Before it transfer the information, it can send mobile node to the neighboring agent and it collect all the information atlast it return back to the network and it calls classifier rule to check out the hackers. If any suspicious activity was found, then it will not forward the message to neighboring node.

3) *Data collection*:

Data collection module is included for every anomaly detection system to collect the information of nodes and values of features for the corresponding layer in a system. Normal profile is created during the normal collection scenario. Attack related data is collected during the attack scenario.

4) *Data process*:

The audit data is collected and record in a file format, so that it can be used for any type of anomaly detection. Data preprocess collection is a technique to process the information with some test train data. In the entire layer misuse detection systems, the previous mentioned preprocessing technique was used.

IV. RESULTS ANALYSIS

The simulation results were conducted with the help of the Network Simulator. The network is running on a laptop with intel3 core, Processor CPU and memory 3-GB RAM. The intention is to provide simulation results and make it easier to compare the results. In NS 2, the nominal configuration has 40 nodes in a flat space. The physical layer and the MAC layer are included in NS2 for providing a platform and make communication with neighbor nodes. The moving speed of mobile node is upto to 30 m/s and a pause time of 1000 seconds. User Datagram Protocol with constant bit rate is implemented with a 512 B packet size of. In order to measure and compare the performance of proposed scheme, consider the following two parameters. Packet delivery ratio (PDR)**:** Packet Delivery Ratio defines the ratio between the number of packets received by the target node and the number of packets sent by the source initiator node. Routing overhead (RO)**:** Routing Overhead defines the ratio between the amount of routing transmissions and with the routing related transmissions such as Route Request packet and Route Reply packet. The comparison graph has been plotted between the malicious nodes and Packet Delivery Ratio.

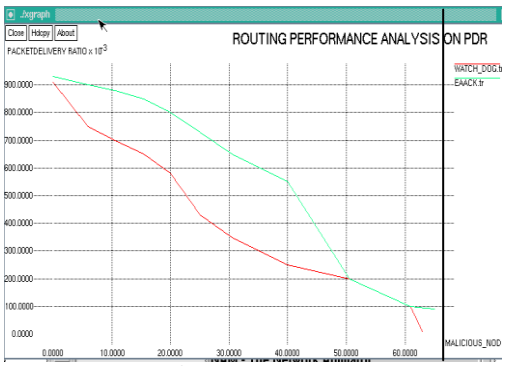

Fig3: Performance analysis on PDR

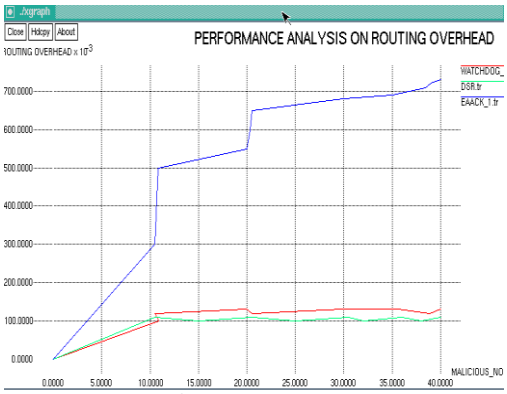

Fig4: Performance analysis on RO

V. CONCLUSION

Packet-dropping attack and collision attack has always created major threat to the security in MANETs. To ensure the security from hackers, we extended our research work to incorporate digital signature for transmitting the data packet as well as the acknowledgement packets. Even though it will create more Routing Overhead in some cases, it can improve the overall network Packet Delivery Ratio when the hackers are smart enough to forge Packets [12]. To achieve optimal results in this network, we can include both Digital Signature Algorithm and Rivest Shamir Adleman algorithm in our simulation. In the future we will extend by implement the hybrid cryptography techniques are to reduce the network overhead caused by digital

Signature. In addition to that we can test the performance of S-ACK in real network environment instead of Simulating in software. At last we will eliminate the requirement of pre-distributed Keys between the nodes.

Acknowledgement

First of all we thank the almighty for giving us the knowledge and courage to complete the research work successfully. I express our gratitude to my respected Professor and Head of CSE Dr R.Ravi M.E.,Ph.D., for following me to do research work intentially.

References

1. M.Elhadi ,Shakshuki, , Nan Kang and R.Tarek Sheltami, 'EAACK—A Secure Intrusion-Detection System for MANETs', IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.
2. A.Ahmed Mohamed Abdalla , H.Ahmad Almazeed, Imane Aly Saroit and Amira Kotb 'Detection and Isolation of Packet Dropping Attacker in MANETs' International Journal of Advanced Computer Science and Applications, Vol. 4, No. 4, 2013.
3. K.Al Agha, M.H Bertin , T. Dang , A. Guitton , P. Minet , T. Val and J.B Viollet , 'Which wireless technology for industrial wireless sensor networks? The development of OCARI technol,' IEEE Transaction Industrial Electronics,Vol. 56, No. 10, pp. 4266–4278, 2009.
4. Alireza Shahrbanoonezhad, Dina Sadat Jalali, and Ali Harounabadi , 'A Hybrid System For Detecting Misbehaving Nodes In Adhoc Networks' International Journal of Information and Electronics Engineering, Vol. 2, No. 3, 2012.
5. T.Anantvalee and J. Wu , 'A Survey on Intrusion Detection in Mobile Ad Hoc Networks' in Wireless/Mobile Security. New York: Springer-Verlag, 2008.
6. L.Buttyan and J.P Hubaux , 'Security and Cooperation in Wireless Networks', Cambridge, U.K, Cambridge University Press, 2007.
7. Y.Hu , D.Johnson and A.Perrig , 'SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks', in Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., pp. 3–13, 2002.
8. D.B Jagannadha Rao , Karnam Sreenu and Parsi Kalpana , 'A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks' International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 8, 2012.
9. Jie Yang, Yingying (Jennifer) Chen, WadeTrappe and Jerry Cheng , 'Detection and Localization of Multiple Spoofing Attackers in Wireless Networks' IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1, 2013.
10. S.Marti , T.JGiuli , K.Lai and M.Baker , 'Mitigating routing misbehavior in mobile ad hoc networks' in Proc. 6th Annu. International Conference on Mobile Computing Networks, Boston, MA, pp. 255–265, 2000.
11. U.Sharmila Begam and G.Murugaboopathi , ' A Recent Secure Intrusion Detection System For Manets' International Journal of Emerging Technology and Advanced Certified Journal, Vol. 3, Special Issue , 2013 .
12. www.google.com

AUTHOR(S) PROFILE

S. Raji is doing M.E Network Engineering in Francis Xavier Engineering college, Tirunelveli. She completed her B.E Electronics and communication Engineering in National Engineering college, Kovilpatti in the year of 2012. She published many Conference Papers. She is an active member in Computer Society of India. Her areas of interest are Network Security, Wireless communication and Mobile Technology.

Dr. R. Ravi is an Editor in International Journal of Security and its Applications (South Korea). He is presently working as a Professor & Head and Research Centre Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He completed his B.E in Computer Science and Engineering from Thiagarajar College of engineering, Madurai in the year 1994 and M.E in Computer Science and Engineering from Jadavpur Government research University, Kolkatta. He has completed his Ph.D in Networks from Anna University Chennai. He has 18 years of experience in teaching as Professor and Head of department in various colleges. He published 12 International Journals, 1 National Journal. He is also a full time recognized guide for various Universities. Currently he is guiding 18 research scholars. His areas of interest are Virtual Private networks, Networks, Natural Language Processing and Cyber security.

