International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 694-705 June 2018-Dec 2018 www.csjournals.com

A Secure IDEA Based AODV routing protocol with an ASACK Scheme for Cluster based Intrusion detection system

[1]Dr.K.Venkatachalapathy, [2]U.Parameshwari, [3]T.Kamaleshwar
[1]Professor & Head, Department of Computer & Information Science, Annamalai University, Chidambaram, India
[2]M.Phil Scholar, Department of Computer & Information Science, Annamalai University, Chidambaram, India
[3]Ph.D. Scholar, Department of Computer Science & Engineering, Annamalai University, Chidambaram, India
[1]omsumeetha@rediffmail.com,[2]paramuuthra55@gmail.com,[3]kamalesh4u2@gmail.com

Abstract: Developing and accessing secure MANET in real scenario is a tedious task that involves a secure design with reduced level of energy consumption. It is necessary one to operate over the continuous node processing system, as mobile nodes are resource constrained. In this project, we make a study about designing a secured cryptographic model. The intention of the study is to efficiently make use of all mobile nodes at the reduced level of energy consumption without compromising the security of nodes. The study is focused into two steps. The first step concentrates on developing an enhanced IDEA cryptography model. And the second step focuses on balancing the loads of IDS nodes in order to reduced energy usage. Our novel proposed systems works independently towards each other under secured environment. Experimental analysis will prove the effectiveness of the system. The limitation and lack of mid monitoring the attacks there are passive and active can be easily following to the MANETs. The Proposed ASACK method helps the supervisor table to increase the speed and efficiency of the networks. Proposal of supervisor table also helps reach the packet to the destination with minimum number of the delays, minimum packet loss, minimum cost when compared to the existing method.

Keywords: IDEA, AODV, ASACK, Intrusion detection

Introduction

Mobile Ad Hoc Network (MANET)

Mobile Ad hoc network is a compiling of self-determining mobile nodes which forms an irregular network without the support of other stand-alone centralized or interactions of administration. Due to the mobility of nodes, the network topology may change quickly and randomly. MANET includes the short radio range and limited bandwidth. In MANET the decentralized network allows the nodes to perform the routing functionalities such as route discovery, topology discovery and delivering messages from source to destination. So, it requires efficient routing technique to send the data from source to destination. In MANETs, mobile stations are free to move around and the network topology changes dynamically. This results in network establishment and breaking of some existing network links due to the fixed transmission range of mobile terminals. Since MANETS are mobile, they use wireless connections like standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission to connect with various networks.

A self organized wireless network is Mobile Ad-hoc Network (MANET) of mobile nodes without any determined infrastructure. Nodes roam through the network, its change to topology quickly and unpredictably over the time. Join the new node for network whereas at the same time for other nodes leave it or just the connections are failed because region to move that is not in the cover range of the network. Node is generally wireless devices such as PDAS, cellular phones or laptops. The very beginning from the use of MANETs has been appealing for all civilian and military applications particularly in the last decade because of wireless LAN technology are developed.

Due to their inherent features of dynamic topology and lack of the centralized management security, MANETs are unprotected to different kinds of attacks. These include passive eavesdropping these impersonating, active interfering and denial-of-service. One of the many possible attacks is BlackHole attack in AODV-based MANETs. This attack a malicious node sends a forged route reply (RREP) packet to source node that initiates route discovery in order to be destination nodes. The AODV protocol stands the compares the source node to destination sequence number contained in RREP packets when receive the source node multiple RREP, it judges the greatest one as the route containing in that RREP packet. Some time the equal for sequence numbers that selects the route with the smallest hop count. The result data transmission flow toward the malicious node by source node and they are dropped.

AODV protocol is ultimate goal of the security solution is to provide security services such as confidentiality, anonymity, authentication and availability to mobile users. Achieve these goals of in order will concentrate in addressing a security concern routing discovery for related and data exchange. Modified protocols are will be proposed that accumulate the routing, private key and session key, authentication, generation and secure exchange of public key. They would be users facilitating to establish parameters are route discovery session during and the parameter would subsequently be used to ensure integrity and confidentiality of data exchange.

AODV Routing Protocol

Ad-hoc On-demand Distance Vector (AODV) is used between source and destination find routing as needed and there are three different types of messages used in this routing protocol such as the route request (RREQ), route reply (RREP) and route error (RRER).

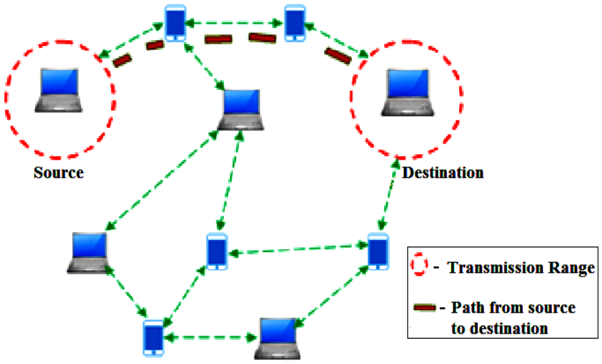


Figure 1. Mobile Ad hoc Network

These messages of information fields such as source IP address, destination IP address, hop count, source and destination sequence number etc,. Every node uses this information which contains in a routing table for specific destination of the routing. Source node wants to communicate with a destination node and there is no any route between them in routing table at the first steps to the source node broadcasts RREQ. Receive the RREQ is intermediate nodes that they are in the range of transmission in the sender. These nodes forward and broadcast this RREQ packet until it is received by the destination or an intermediate node that new enough route to the destination.

After the destination send RREP unicast regarding the source. Accordingly a route among the source and destination is organized. A new enough route is a valid route entry that its sequence number of destination is at least as great as a destination sequence number in RREQ packet. The sequence number of source is used to control freshness about route to be the source. In addition the sequence number of destination is used to determine freshness of a route to the destination. When receive RREP for intermediate with consideration of sequence number of destination and counts of hop, it updates or creates a forward route entry in its routing table for that destination.

Route maintenance procedure keep the nodes an entry for every active route in their routing table and periodically the broadcast Hello message to its neighbors in order to find a possible link failure. If a link failure node detects it knows that each active routes via this link fail. So a Route Error Message (RERR) is sent to announce each relative node of source. The nodes of source then will determine whether to refresh the route or not.

HOW MANET WORKS?

The MANET is the functioning group to improvise the IP routing protocol function, since it is fit for wireless application for both static and dynamic topologies. This is due to node motion and other factors.

Approaches are designed to be comparatively lightweight in nature, appropriate for multiple hardware and wireless atmosphere, and address scenarios where MANETs are arranged at the edges of an IP infrastructure. Also by MANET specifications and management features it should support Hybrid mesh infrastructures (e.g., a mixture of fixed and mobile routers).

The WG will develop two Standards track routing protocol specifications using established components from previous work on experimental reactive and proactive protocols.

- Reactive MANET Protocol(RMP)
- Proactive MANET Protocol(PMP)

The WG may decide to go with converge approach, when the significant unity between RMRP and PMRP protocol modules is observed. Both IPv4 and IPv6 will be supported as well as the routing security requirements and issues will also be addressed. The MANET WG will also develop a protocol that can efficiently forward overflow data packets to all participating MANET nodes. The main purpose of this mechanism is a simplified best effort multicast forwarding function. The use of this protocol is designed to be applied only within MANET routing areas and the WG effort will be limited to routing layer design issues. The MANET WG will focus to the OSPF-MANET protocol, which work within the OSPF WG and IRTF which is towards research topics related to MANET field.

The WG may choose to run with focalize approach, when the noteworthy solidarity amongst RMRP and PMRP convention modules is watched. Both IPv4 and IPv6 will be upheld and additionally the directing security prerequisites and issues will likewise be tended to. The MANET WG will likewise build up a convention that can effectively forward flood information bundles to all partaking MANET hubs. The fundamental reason for this system is a streamlined best exertion multicast sending capacity. The utilization of this convention is intended to be connected just inside MANET steering territories and the WG exertion will be restricted to directing layer configuration issues. The MANET WG will focus on the OSPF-MANET convention work inside the OSPF WG and IRTF work which is tending to investigate points identified with MANET conditions.

Literature Survey

S. Marti, T. J. Giuli, K. La and M. Baker[1] This paper portrays two systems that enhance throughput in a specially appointed system within the sight of hubs that consent to forward parcels however neglect to do as such. To alleviate this issue, we propose arranging hubs in view of their progressively estimated conduct. We utilize a guard dog that distinguishes acting up hubs and a way rater that aides directing conventions keep away from these hubs. Through reenactment we assess guard dog and way rater utilizing bundle throughput, level of overhead (directing) transmissions, and the precision of getting out of hand hub identification. At the point when utilized together in a system with direct portability, the two methods increment throughput by 17% within the sight of 40% getting rowdy hubs, while expanding the level of overhead transmissions from the standard steering convention's 9% to 17%. Amid outrageous versatility, guard dog and way rater can expand organize throughput by 27%, while expanding the overhead transmissions from the standard directing convention's 12% to 24%.

N. Marchang and R. Datta[2] Mobile ad hoc networks (MANETs) were originally designed for a cooperative environment. To use them in hostile environments, trust-based routing can be used, where instead of establishing the shortest routes as done in traditional routing protocols, most trusted routes are established. In this study, the authors present a light-weight trust-based routing protocol. It is light-weight in the sense that the intrusion detection system (IDS) used for estimating the trust that one node has for another, consumes limited computational resource. Moreover, it uses only local information thereby ensuring scalability. Our light-weight IDS takes care of two kinds of attacks, namely, the blackhole attack and the grey hole attack. Whereas our proposed approach can be incorporated in any routing protocol, the authors have used AODV as the base routing protocol to evaluate our proposed approach and give a performance analysis.

I. Khalil, S. Bagchi and N. B. Shroff [3]Sleep-wake conventions are basic in sensor systems to guarantee seemingly perpetual task. In any case, an open issue is the manner by which to create productive systems that can be fused with rest wake conventions to guarantee both extensive activity and a high level of security. Our commitment in this paper is to address this issue by utilizing neighborhood checking, an intense system for distinguishing and moderating control and information assaults in sensor systems. In nearby observing, every hub regulates some portion of the movement going all through its neighbor's to decide whether the conduct is suspicious, for example, surprisingly long postponement in sending a bundle. Here, we show a convention called SLAM to make nearby observing closefisted in its vitality utilization and to coordinate it with any surviving rest wake convention in the system. The test is to empower rest wake in a protected way even notwithstanding hubs that might be ill-disposed and not wake up hubs in charge of observing its movement. We demonstrate scientifically that the security scope isn't debilitated by the convention. We perform recreations in ns-2 to exhibit that the execution of nearby observing is essentially unaltered while listening vitality sparing of 30 to 129 times is accomplished, contingent upon the system stack.

R. Zheng, T. Le and Z. Han[4] We consider the issue of ideally choosing m out of M sniffers and relegating every sniffer one of the K channels to screen the transmission exercises in a multi-channel remote system. The movement of clients is at first obscure to the sniffers and is to be learned alongside channel task choices. Indeed, even with the full information of client action measurements, the disconnected improvement issue is known to be NP-hard. In this paper, we initially propose an incorporated online estimate calculation and demonstrate that it acquires sub-direct lament limits after some time. A conveyed calculation is then proposed with direct message multifaceted nature. We exhibit both scientifically and exactly the exchange offs between the calculation cost and the rate of learning.

D. B. Johnson and D. A. Maltz[5] A specially appointed system is an accumulation of remote versatile hosts shaping a transitory system without the guide of any settled foundation or brought together organization. In such a situation, it might be important for one versatile host to enroll the guide of different has in sending a parcel to its goal, because of the restricted scope of every portable host's remote transmissions. This paper shows a convention for directing in specially appointed systems that utilizations dynamic source steering. The convention adjusts rapidly to directing changes when have development is visit, yet requires practically zero overhead amid periods in which has move less as often as possible. In light of results from a parcel level reproduction of portable hosts working in a specially appointed system, the convention performs well finished an assortment of natural conditions, for example, have thickness and development rates. For everything except the most elevated rates of host development reenacted, the overhead of the convention is very low, tumbling to only 1% of aggregate information bundles transmitted for direct development rates in a system of 24 versatile hosts. In all cases, the distinction long between the courses utilized and the ideal course lengths is unimportant, and much of the time, course lengths are all things considered inside a factor of ideal.

Sergio Marti et al were they proposed the basic model for intrusion detection system called as Watchdog technique [7].In Watchdog framework, it distinguishes the malicious hub and neglected to concur the forward the data packets in MANET. Because of the crash, collision, restricted transmission control, false malicious reporting and fractional dropping the Watch Dog may neglected to recognize the nearness of Malicious Node. Path rater is the next proposed work, were this technique used in the routing protocol in order to pass up the malicious node. Parker et al was developed the extended version of watchdog called ExWatchdog (Enhanced Watchdog) that was give alert on the malicious node, it is the extended version of Watchdog [8]. It maintains the routing table in order to notice the count of packet sent and received correspondingly. The Route guard, it is a novel intrusion detection and also reply system, it is combination of both techniques Path rater and Watchdog [9]. This type of techniques were comes under the active response and also passive response manner. Sonja Bunchegger et al was proposed a method called Cooperation of Nodes Fairness in Dynamic Adhoc networks (CONFIDENT) , in this every node contains in the network that maintains a four main components like a trust manager, reputation, path and a monitor[11]. Cooperation Enhancement in Manet that was developed for maintain the malicious node by restrictive the number of packets that are forwarded [11].

The watch dog methods are simpler and base for the all other methods. The TWOACK is proposed by Balakrishnan et al [16] that replaces Watchdog and solves the problem of the receiver collision and limited transmission power. This scheme is used in source routing protocol. In TWOACK each forwarded packet has to be acknowledged. The AACK is considered as Enhanced TWOACK aims to improve the performance of TWOACK proposed by Shakshuki et al [17]. To detect the selfish Gunasekaren et al[18]as AAS(Authenticated Acknowledgement Scheme).Those selfish nodes were eliminated and networks is free from intrusions. Selfish node only send the packets to destination that could not focussed on the neighbour node.

The above two methods are simple and that are base for all other technique. Balakrishnan et all proposed a TWOACK that will replace the Watchdog and give remedy for the collision and also transmission power [13].

The EAACK (Enhanced Adaptive Acknowledgement) was proposed by Nankang et al [19] are bidirectional. The EAACK scheme mainly classified into 1.ACK 2.SACK 3. MRA.

Table 1.EAACK scheme

Packet Flag	Packet Type
01	Acknowledgement
10	Selective Acknowledgment
11	Misbehavior Report Authentication

The EAACK can detect the malicious node with the fake misbehaving report. Also it sends the Acknowledgement (ACK) and No acknowledgement (Nack) to previous nodes whenever the packets reaches the destination. Along with that it has both S-Ack and MRA to send the report of the node status.

Feature

Cooperative game theory can be used in model situations in which players coordinate their strategies and share the payoffs between them. The output of the game (individual payoffs that players receive) must be in equilibrium so that no player has incentive to break away from the coalition .The game settings in all the earlier game-theoretic work on IDS involves two sets of opposing players, the nodes/IDSs and the attacker/defaulters. In our work, we have set a game that involves players (IDSs sitting in neighbouring nodes) cooperating to achieve a common goal (i.e., to monitor a single node). To the best of our knowledge, we have not come across any work on cooperating IDSs (to get a security versus energy trade-off) that models such a situation using game theory. We have presented such a cooperative multi-player game to model the interactions between the IDSs in a neighbourhood and used it to validate our proposed probabilistic scheme.

The contributions of this paper are summarized as follows:

A study about designing a secured cryptographic model. The intention of the study is to efficiently make use of all mobile nodes at the reduced level of energy consumption without compromising the security of nodes. The study is focused into two steps. The first step concentrates on developing an enhanced IDEA cryptography model. And the second step focuses on balancing the loads of IDS nodes in order to reduced energy usage. Our novel proposed systems works independently towards each other under secured environment. The proposed scheme uses local information, thus making it distributed and scalable. Moreover, it works on both static and mobile networks.

Proposed System

In this project, we make a study about designing a secured cryptographic model. The objective of the study is to efficiently make use of all mobile nodes at the reduced level of energy consumption without compromising the security of nodes. The study is focused into two steps. The first step concentrates on developing an enhanced IDEA cryptography model and the second step focuses on balancing the loads of IDS nodes in order to reduced energy usage. Our novel proposed systems works independently towards each other under secured environment. Experimental analysis will prove the effectiveness of the system.

Implementation

(i) Topology Creation

In our imitation, the 50 number of sensor nodes are arranged. They are randomly arranged in a region with the size of 2000 X 1500. Data packets are generated in each sensor according to a Poisson process with the same parameter to very low traffic load; to simulate a mobile network scenario. We set the speed range from max 5 m/s to min 2.70 m/s. The nodes are having a 250 m of transmission range (rc) and a 50 kbps of data rate. The size of the packet is determined by the size of the data payload and by the space required to include the information of the next hop forwarder set. We have considered that the data packets have a payload of 150 bytes.

(ii) IDEA Cryptography

The IDEA is not at all like the other piece figure calculations examined in this area is obtained by the Swiss firm of Ascom. They have, however, been generous in allowing, with permission, free non commercial use of their algorithm, with the result that IDEA is best known as the block cipher algorithm used within the popular encryption program PGP. The IDEA calculation is fascinating in its own particular right. It incorporates few stages; to start with, it makes create the impression that it may be a non-invertible hash work rather than a square figure. Next, it entirely avoids the use of any lookup tables or S-boxes. They are 52 sub keys uses in IDEA, both 16 bits long. Two are used during every round proper, and four are used before each round and then the final round. It is having the eight rounds.

The plaintext of block in IDEA is classified into four quarters, every 16 bits longs. There are three operation are Addition, XOR and multiplication are used in IDEA to conflate two 16 bit values to acquire 16 bit result. 1 Addition is normal addition with carries, modulo 65,536. As used in IDEA, Multiplication requires some explanation. Multiplication zero always produces the zero, and is not invertible. In case of the multiplication modulo n is also not a invertible ,where is not a relatively prime to n when it is by a number. The way multiplication is used in IDEA, is necessary that it be always invertible. This is true of multiplication IDEA style. The number 65,537, when is 2^16+1, is a number 65,537 prime number. (Aprox, 2^8+1, is always prime, and so is 2^4+1, but 2^32+1 is a not prime, so the IDEA cannot be negligibly insignificantly rescaled up to a 128-bit block size.) Thus, if one forms a multiplication table for the numbers from 1 through 65,536, each row and column will contain every number only once, forming a Latin square, and providing an invertible operation. The numbers are from 0 to 65,535 from the formation of 16 bits. The purpose of multiplication in IDEA, a 16 bit words containing its considered the every zeros is to represent to the number 65,536; further numbers are represented to in conventional unsigned notations, and the modulo of multiplication is the prime number 65,537.

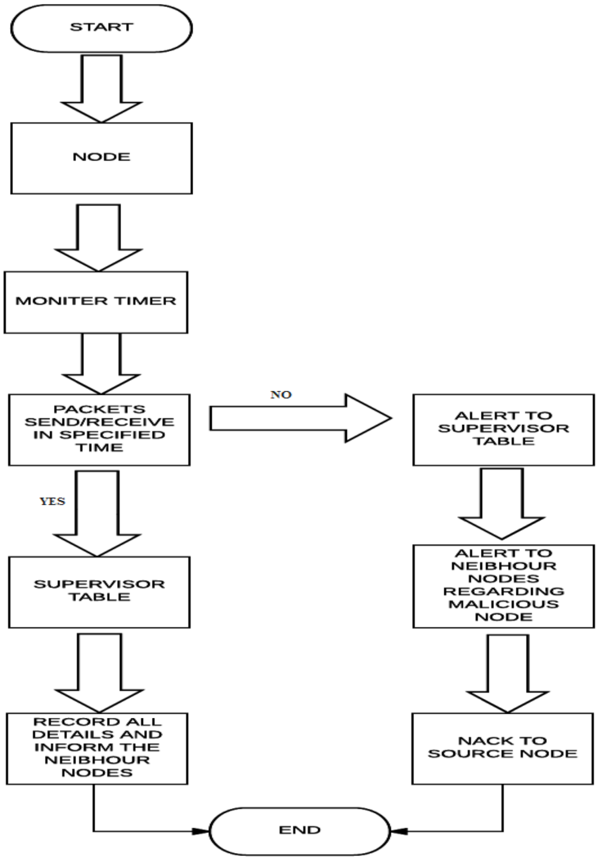
(iii) Black hole /Grey hole Attack

Black hole attacks are a routing layer attacks in which the data are revolves from the other node. The packets transmission on multiple nodes and packet dropping is mostly route layer in occurring. It was targeted to the routing protocol by the attack. Great influencing attacks in black hole attack on virtual mesh networks. Difficult to detect attack is black hole attack, there mostly found in the temporary networks like wireless/virtual mesh networks. Black hole attack is busy DOS attack. Powerful effect in grey hole attack to the performance of mesh network. Grey hole attack the sender node reply the receive messages from malicious node and smallest way make to receivers nodes. Reply message sends the malicious node after authorized node to sender node and then the sender node become confuse in two replies. The malicious node becomes the sender node and whole data are received by it. The data packets are fully dropped the sender node.

The sender node 1 sends the large amount of PREQ messages to all nearby nodes. When RREQ messages are received by the malicious nodes, then it sends RREP message to the sender node which is non-real and also show the shortest way to reach to the receiver node. Then accepts the sender nodes for reply message from non-real node that is called malicious node and transfers the packets. This attacks are known as grey hole attack.

(iv) ASACK

Maintain the information about the node and packets to help the supervisor node whether it receive from the promiscuous node or malicious node. The packets once the node receives from the neighbor nodes supervisor table to be check and neighbour node to be verifies is original or malicious. The original node it again forward to the packet and save that the node is not a malicious. It is malicious and doesn’t match to the monitoring timer neighbour from the packets sends the NACK back and send the suspect alert to its neighbor.


START
NODE
MONITER TIMER
PACKETS SEND/RECEIVE IN SPECIFIED TIME
NO
ALERT TO SUPERVISOR TABLE
YES
SUPERVISOR TABLE
ALERT TO NEIBHOUR NODES REGARDING MALICIOUS NODE
RECORD ALL DETAILS AND INFORM THE NEIBHOUR NODES
NACK TO SOURCE NODE
END

Every node Mean in the deviation results are finding the difference to estimated with estimated and actual values. The actual and the expected value of help to difference value to find of the node. We have to calculate the mean, standard deviation, variance, expected value where the expected value is calculates to using formula is (mean+variance). The difference value is the greater then the threshold values that fount the node as the malicious as well it is safer node.

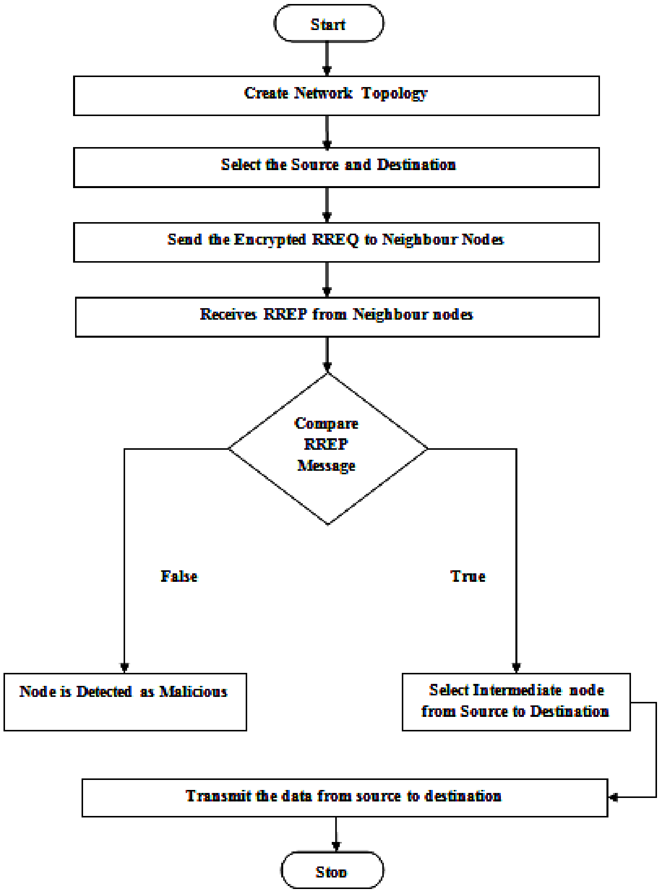
We use probability based identify the clustering relationship between the values. Comparing the values with threshold value we are find to the malicious node. The relationship is to estimated with three there are standard deviation, mean, sampling probability. The defining of mean is µA and defining of standard deviation is σA. Samples are chosen to the probability of A.

We can result to the normalized with their sum. The value of normalized with the value of expected is upper bound after it is said to be malicious node. The network efficiency will increase when the compare to number of nodes at a single time.

Performance Evaluation

In this section, the performance of simulation is evaluated. We are using the xgraph for evaluating the performance. We choose some evaluation metrics: Packet delivery ratio – the ratio of the total number of packets received by the destination node to the number of packet sent by the source, End-to-End delay – the time taken to be data transmitted from source node to destination node. And calculate the Energy consumption by the sensor node. Along with these evaluation metrics we have to evaluate the simulation performance in xgraph.

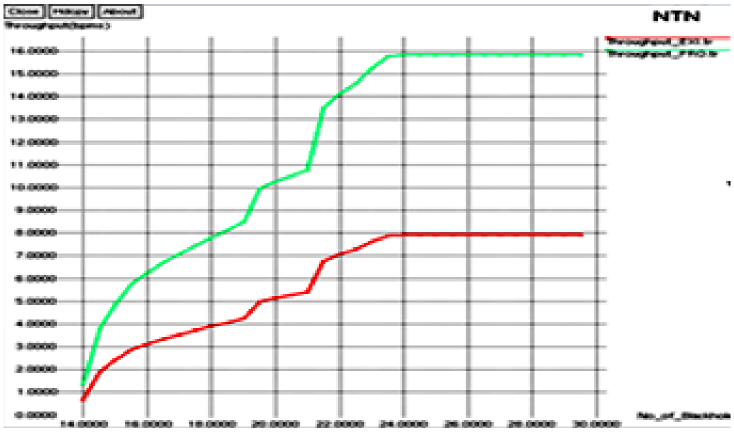
System work flow


Start
Create Network Topology
Select the Source and Destination
Send the Encrypted RREQ to Neighbour Nodes
Receives RREP from Neighbour nodes
Compare RREP Message
False
True
Node is Detected as Malicious
Select Intermediate node from Source to Destination
Transmit the data from source to destination
Stop

The system flow is represented using the above flow chart. In MANET the network topology is created to transfer the data packets from source to destination. Once the date packet is ready to transfer, the source and the destination will be selected. During this communication process, the sender node sends the encrypted RREQ (Response Request) to the neighbour nodes. When the RREQ is received by the neighbour nodes, the RREP (Request Response) is received by the sender node.

The received RREP messages from the neighbour nodes are compared to check to identify the malicious nodes. If the malicious node is detected, it is represented as FALSE and if the malicious node is not detected it is represented as TRUE. If the network path is TRUE then the source and destination nodes are selected to transfer the data packets. There will be no attack and the message was flow to the final destination with acknowledgment.

Simulation results



This shows the comparison result of throughput between the existing and the proposed work. The IDEA cryptography with ASACK which gives better result, when compare to the existing one.

Conclusion

Nowadays, the security management in Mobile Ad hoc Networks is widely studied by the researchers. Energy Utilization is the most vital part in the node communication systems. The concept of security is important to communication and network protocol designers where establishing secured relationships among participating nodes is critical to enabling collaborative optimization of system metrics. In this thesis, we explored an energy utilization mechanism in the trusted Mobile Ad hoc Networks. The study is focused into two steps. The first step concentrates on developing an enhanced IDEA cryptography model. And the second step focuses on balancing the loads of IDS nodes in order to reduced energy usage. Our novel proposed systems works independently towards each other under secured environment. Experimental analysis will prove the effectiveness of the system. MANET of the performance may decrease when occurs of misbehavior node and that leads to route failure. The Intrusion Detection System through probability based to the clustering is proposed for the malicious nodes are identifying. This method will help to the increasing detecting speed the malicious node and delivery of the packet may increase without overhead. Since helps to the Network Simulator is show the result and view the graph cleverly. The performance of network is increased when compared to the existing methods.

References

[1] S. Zeadally , R. Hunt, Y-S. Chen, A. Irwin and A. Hassan, ”Vehicular adhoc networks (VANETS): status, results, and challenges,” Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2012.

[2] S. K. Bhoi and P. M. Khilar, ”Vehicular communication: a survey”, IET Networks, vol. 3, no. 3, pp. 204 - 217, 2014.

[3] S. Marti, T. J. Giuli, K. La and M. Baker, ”Mitigating Routing Misbe-havior in a Mobile Ad-hoc Environment,” Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255-265, August 2000.

[4] C. Manikopoulos and L. Ling, ”Architecture of the Mobile Ad-hoc Network Security (MANS) System,” Proc. IEEE International Conference on Systems, Man and Cybernetics, vol. 4, pp. 3122- 3127, October 2003.

[5] K. Nadkarni and A. Mishra, ”Intrusion Detection in MANETs – The Second Wall of Defense,” Proc. IEEE Industrial Electronics Society Conference ’2003, pp. 1235-1239, Roanoke, Virginia, USA, Nov. 2-6, 2003.

[6] A. Partwardan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis, ”Secure Routing and Intrusion Detection in Ad-hoc Networks,” Proc. 3rd IEEE International Conference on Pervasive Computing and Communications,Hawaii Island, Hawaii, March 8-12, 2005.

[7] N. Marchang and R. Datta, ”Lightweight Trust-based Routing Protocol for Mobile Ad Hoc Networks,” IET Information Security, vol. 6, no. 4, pp. 77-83, 2012.

[8] N. Marchang and R. Datta, ”Collaborative Techniques for Intrusion Detection in Mobile Ad-hoc Networks,” Elsevier Ad Hoc Networks, vol.6, no. 4, pp. 508-523, June 2008.

[9] D. Dong, X. Liao, Y. Liu, C. Shen and X. Wang, ”Edge Self-Monitoring for Wireless Sensor Networks,” IEEE Transactions on Parallel and Dis-tributed Systems,” vol. 22, no. 3, March 2011, pp. 514-527.

[10] I. Khalil, S. Bagchi and N. B. Shroff, ”SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks,” Proc. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2007 (DSN 2007), 565-574.

[11] T. Hoang Hai and E-N. Huh, ”Optimal Selection and Activation of Intrusion Detection Agents for Wireless Sensor Networks,” Proc. Future Generation Communication and Networking (FGCN 2007), vol.1, no., pp.350-355, 6-8 Dec. 2007.

[12] S. M. Fitaci, K. Jaffres-Runser and C. Comaniciu, ”On modeling energy-security trade-offs for distributed monitoring in wireless ad hoc networks,” Proc. Military Communications Conference, 2008. MILCOM 2008. IEEE , vol., no., pp.1-7, 16-19 Nov. 2008.

[13] R. G. Clegg, S. Clayman, G. Pavlou, L. Mamatas and A. Galis, ”On the Selection of Management/Monitoring Nodes in Highly Dynamic Networks,” IEEE Transactions on Computers, vol.62, no.6, pp.1207-1220, June 2013.

[14] R. Zheng, T. Le and Z. Han, ”Approximate Online Learning Algorithms for Optimal Monitoring in Multi-Channel Wireless Networks,” IEEE Transactions on Wireless Communications, vol.13, no.2, pp.1023-1033, February 2014.

[15] N. Tsikoudis, A. Papadogiannakis and E. P. Markatos, ”LEoNIDS: a Low-latency and Energy-efficient Network-level Intrusion Detection System,” IEEE Transactions on Emerging Topics in Computing, Vol. PP, no. 99, 2014.

[16] R. Muradore and D. Quaglia, ”Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security,” IEEE Transactions on Industrial Informatics, Vol. 11, no. 3, pp. 830-840, 2015.

[17] S. Shen, ”A game-theoretic approach for optimizing intrusion detection strategy in WSNs,” Proc. 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), pp.4510-4513, 8-10 Aug. 2011.

[18] A. Afgah and S. K. Das and K. Basu, ”A Non-cooperative Game Approach for Intrusion Detection in Sensor Networks,” Proc. VTC 2004, Fall 2004.

[19] T. Alpcan and T. Basar, ”A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection,” Proc. 43rd IEEE Conference on Decision and Control, December 2004.

[20] Y. Liu, H. Man and C. Comaniciu, ”A Game Theoretic Approach to Efficient Mixed Strategies for Intrusion Detection,” Proc. IEEE International Conference on Communications (ICC 2006), 2006.

[21] Y. Liu, C. Comaniciu and H. Man, ”ModelingMisbehavior in AdHoc Networks: A Game Theoretic Approach for Intrusion Detection,” International Journal of Security and Networks, vol. 1, no. 3-4, 2006.

[22] L. Chen and Jean Leneutre, ”A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks,” IEEE Transactions of Information Forensics and Security, vol. 4, no. 2, June 2009.

[23] A. Patcha and J. Park, ”A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks,” International Journal of Network Security, vol. 2, no. 2, pp. 146-152, March 2006.

[24] N. Zhang, W. Yu, X. Fu and S. K. Das, ”Maintaining Defender’s Repu-tation in Anomaly Detection Against Insider Attacks,” IEEE Transactions on Systems, Man, and Cybernetics-Part B:Cybernetics, vol 40, no. 3, June2010, pp. 597-611.

[25] P. Michiardi and R. Molva, ”A Game Theoretical Approach to Evaluate Cooperation Enforcement Mechanisms in Mobile Ad Hoc Networks,” Proc. WiOpt 2003: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, March 2003.