Improving The Node Efficiency Using Cryptographic Technique

M. Aathithyan[1], Dr. R. Bhavani[2], Dr. R. Priya[3]
[1, 2, 3] Dept. of CSE
[1, 2, 3] Annamalai University

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 reduce energy usage. Our novel proposed systems works independently towards each other under secured environment. Experimental analysis will prove the effectiveness of the system.*

Keywords- MANET, IDEA, IDS.

I. INTRODUCTION

A. Mobile Ad Hoc Network

Mobile Ad hoc network is a collection of independent mobile nodes forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. The network topology may change quickly and randomly due to mobility of nodes. MANET contains short radio range and limited bandwidth. Also, in MANET the decentralized network leads to perform the routing functionalities by nodes themselves such as route discovery, topology discovery and delivering messages from source to destination. So, it requires efficient routing method to send the data packet from source to destination as much as possible. Mobile stations in MANETs are free to move around.

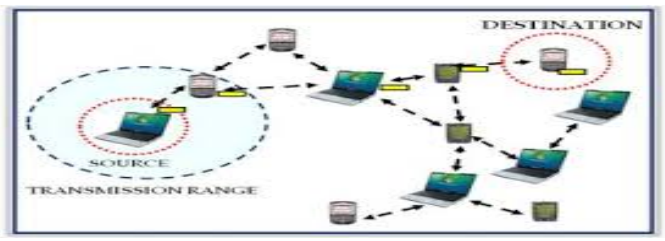

Figure 1. Mobile Ad hoc Network

Because of the fixed transmission range of mobile terminals, the network topology changes dynamically resulting in network establishment and breaking of some existing network links. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. Figure 1.1 represents the architecture of Mobile Ad Hoc Network.

B. How Manet Works?

The purpose of the MANET working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion and other factors.

Approaches are intended to be relatively light weight in nature are suitable for multiple hardware and wireless environments, and address scenarios where MANETs are deployed at the edges of an IP infrastructure.

Hybrid mesh infrastructure (e.g. a mixture of fixed and mobile routers) should also be supported by the MANET specifications and management features.

Using mature components from previous work on experimental reactive and proactive protocols, the Working Group (WG) will develop two Standards track routing protocol specifications:

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

If significant commonality between Reactive MANET Protocol (RMP) and Proactive MANET Protocol (PMP) modules is observed, the WG may decide to go with a converged approach. Both IPv4 and IPv6 will be supported. Routing security requirements and issues will also be addressed. The MANET WG will also develop a scoped forwarding protocol that can efficiently flood data packets to all participating MANET nodes. The primary purpose of this mechanism is a simplified best effort multicast forwarding

function. The use of this protocol is intended to be applied only within MANET routing areas and the WG effort will be limited to routing layer design issues. The MANET WG will pay attention to the OSPF-MANET protocol work within the OSPF WG and IRTF work that is addressing research topics related to MANET environments.

II. LITERATURE REVIEW

S. Marti, T. J. Giuli, K. La and M. Baker [1] This paper describes two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, categorizing nodes based upon their dynamically measured behaviour method is proposed. A watchdog that identifies misbehaving nodes and a path rater that helps routing protocols avoid these nodes. Through simulation, evaluate watchdog and path rater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and path rater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol'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 black hole 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 protocols are critical in sensor networks to ensure long-lived operation. However, an open problem is how to develop efficient mechanisms that can be incorporated with sleep-wake protocols to ensure both long-lived operation and a high degree of security. Our contribution in this paper is to address this problem by using local monitoring, a powerful technique for detecting and mitigating control and data attacks in sensor networks. In local monitoring, each node oversees part of the traffic going in and out of its neighbour's to determine if the behaviour is suspicious, such as, unusually long delay in forwarding a packet. Here, we present a protocol called SLAM to make local monitoring parsimonious in its energy consumption and to integrate it with any extant sleep-wake protocol in the network. The challenge is to enable sleep-wake in a secure manner even in the face of nodes that may be adversarial and not wake up nodes responsible for monitoring its traffic. It is proved analytically that the security coverage is not weakened by the protocol. The performance of simulations in ns-2 to demonstrate that local monitoring is practically unchanged while listening energy saving of 30 to 129 times is achieved, depending on the network load.

R. Zheng, T. Le and Z. Han [4] The problem of optimally selecting m out of M sniffers and assigning each sniffer one of the K channels to monitor the transmission activities in a multi-channel wireless network. The activity of users is initially unknown to the sniffers and is to be learned along with channel assignment decisions. Even with the full knowledge of user activity statistics, the offline optimization problem is known to be NP-hard. In this paper, a centralized online approximation algorithm and show that it incurs sub-linear regret bounds over time. A distributed algorithm is then proposed with moderate message complexity. The trade-offs between the computation cost and the rate of learning is demonstrated both analytically and empirically.

B. Johnson and D. A. Maltz [5] An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. This paper presents a protocol for routing in ad hoc networks that uses dynamic source routing. The protocol adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently. Based on results from a packet level simulation of mobile hosts operating in an ad hoc network, the protocol performs well over a variety of environmental conditions such as host density and movement rates. For all but the highest rates of host movement simulated, the overhead of the protocol is quite low, falling to just 1% of total data packets transmitted for moderate movement rates in a network of 24 mobile hosts. In all cases, the difference in length between the routes used and the optimal route lengths is negligible, and in

most cases, route lengths are on average within a factor of optimal.

III. PROPOSED SYSTEM

In this paper, 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.

Cooperative game theory can be used to 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.

IV. IMPLEMENTATION

A. Topology Creation

In our simulations, the 50 number of sensor nodes are deployed. They are randomly deployed in a region the size of 2000 X 1500. In each sensor, data packets are generated 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 have a transmission range (rc) of 250 m and a data rate of 50 kbps. 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 consider that data packets have a payload of 150 bytes.

B. IDEA Cryptography

IDEA, unlike the other block cipher algorithms discussed in this section, is patented 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 algorithm is interesting in its own right. It includes some steps which, at first, make it appear that it might be a non-invertible hash function instead of a block cipher. Also, it is interesting in that it entirely avoids the use of any lookup tables or S-boxes. IDEA uses 52 sub keys, each 16 bits long. Two are used during each round proper, and four are used before every round and after the last round. It has eight rounds.

The plaintext block in IDEA is divided into four quarters, each 16 bits long. Three operations are used in IDEA to combine two 16 bit values to produce a 16 bit result, addition, XOR, and multiplication. Addition is normal addition with carries, modulo 65,536. Multiplication, as used in IDEA, requires some explanation. Multiplication by zero always produces zero, and is not invertible. Multiplication modulo n is also not invertible whenever it is by a number which is not relatively prime to n. The way multiplication is used in IDEA, it is necessary that it be always invertible. This is true of multiplication IDEA style. The number 65,537, which is 2^16+1, is a prime number. (Incidentally, 2^8+1, or 257, is also prime, and so is 2^4+1, or 17, but 2^32+1 is not prime, so IDEA cannot be trivially scaled 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 once only, forming a Latin square, and providing an invertible operation. The numbers that 16 bits normally represent are from 0 to 65,535 (or, perhaps even

more commonly, from -32,768 to 32,767). In IDEA, for purposes of multiplication, a 16 bit word containing all zeroes is considered to represent the number 65,536; other numbers are represented in conventional unsigned notation, and multiplication is modulo the prime number 65,537.

C. Black hole /Grey hole Attack

Black hole attack is a routing layer attack in which data is revolves from other node. The transmission of packets on multiple nodes and dropping of packets is mostly occurring on routing layer. Routing protocol is targeted by the attack. Black hole attack having great influencing attack on virtual mesh network. The busy DOS attack is black hole attack. Black hole attack is difficult to detect; it is mostly found in temporary networks like virtual/wireless mesh networks. Grey hole attack will cause powerful effect to the performance of mesh networks. In grey hole attack, the sender node receive reply message from malicious node and make smallest way to receiver node. Malicious node sends reply message after authorized node to sender node and then sender become confuse in two replies. On that way, malicious node becomes sender node and whole data received by it. In this, the data packets fully dropped by sender node. In the scenario, the sender node 1 sends large amount of RREQ message to every nearby nodes. When RREQ message is received by malicious node, then it sends RREP message to sender node which is non-real and also shows the shortest way to reach to receiver node. Then sender node accepts the reply message from non-real node which is called malicious node and transfers the packets. This attack is known as grey hole attack.

D. Performance Evaluation

In this section, performance of simulation was evaluated. To evaluate the performance xgraph is used. Some of the evaluation matrices are:

i. Packet delivery ratio-the ratio of the total number of packet received by the destination node to number of packet sent by the source.
ii. End-to-End delay- the time taken to be data transmitted from source node to destination node.
iii. The energy consumption by the sensor node is calculated. Along this the simulation performance in xgraph is evaluated.

V. RESULTS AND DISCUSSION

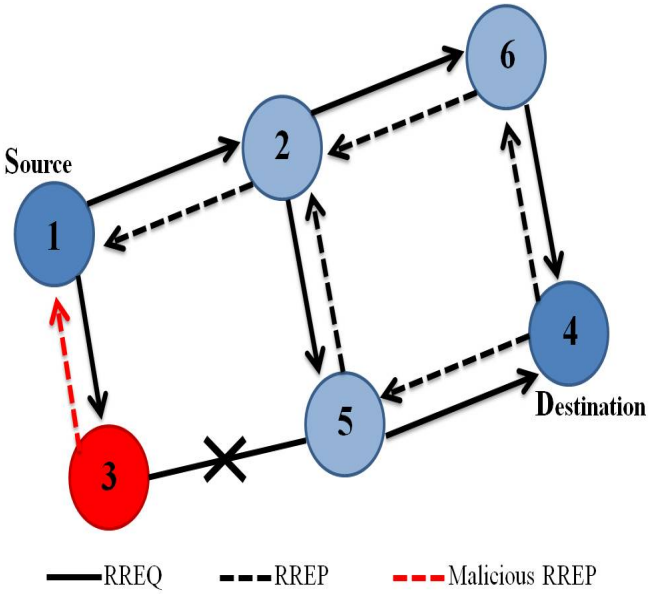

Figure 2. System Architecture

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. Figure 5.1 represents the System Architecture of Mobile Ad Hoc Network.

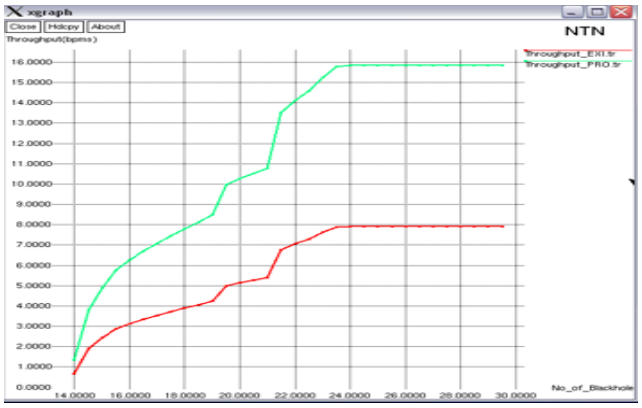

Figure 3. Performance of Throughput

The Figure 5.2 Xgraph reprsents the performancee of throughput and Figure 5.3 represents the performance of routing overhead.

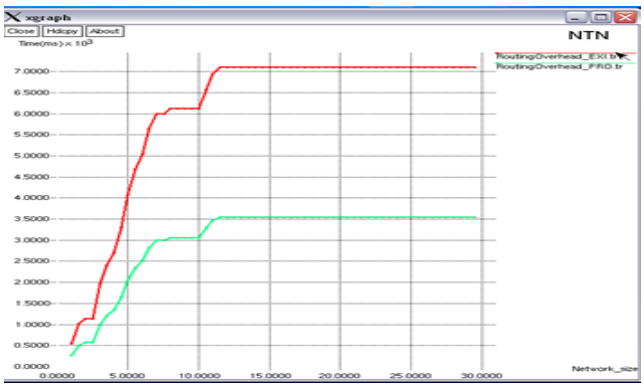

Figure 4. Performance of RoutingOverhead

VI. 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 in communication and network protocol designers where establishing secured relationships among participating nodes is critical to enabling collaborative optimization of system metrics. In this work, 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 reduce energy usage. Our novel proposed systems works independently towards each other under secured environment.

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". 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.