Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.724 – 734

RESEARCH ARTICLE

TRUSTED SYSTEM WITH KERNEL BASED AUTHENTICATION FOR SECURITY ENHANCEMENTS IN MOBILE AD-HOC NETWORKS

Miss. G.Jothimani[1], Mrs. R.Kavitha[2]

[1]M.Phil Research Scholar, Department of Computer Science Vivekanandha College for Women

[2]Assistant Professor in Department of Computer Science Vivekanandha College for Women, Tiruchengodu, Namakkal

[1] jothimani.cs@gmail.com, [2] kavithamscmphil@gmail.com

ABSTRACT— Mobile Ad-hoc Networks (MANETs) are extremely vulnerable to a variety of misbehaviors because of their basic features including lack of communication infrastructure, short transmission range, and dynamic network topology. To detect and mitigate those misbehaviors, many trust management schemes have been proposed for MANETs. Most rely on pre-defined weights to determine how each apparent misbehavior contributes to an overall measure of trustworthiness. The extremely dynamic nature of MANETs makes it difficult, however, to determine a set of weights that are appropriate for all contexts. The trust management scheme for MANETs that uses SATEM for machine learning to classify nodes by its behaviours and identifies whether the nodes as malicious or not. SATEM is far more resilient to the context changes common in MANETs, such as those due to malicious nodes altering their misbehavior patterns over time or rapid changes in environmental factors, such as the motion speed and transmission range. A kernel based SATEM uses a fixed formula to calculate the trustworthiness of mobile nodes in an automated manner. The Dempster-Shafer Theory (DST) which combine separate pieces of observations (evidences) to calculate the probability of malicious behaviors.

1. INTRODUCTION

MANET Stands for "Mobile Ad Hoc Network." A MANET is a type of ad hoc Network that can change locations and configure itself on the fly. 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. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. MANET (Mobile ad hoc network) is an infrastructure less, wireless and self-configuring network of mobile devices. These are mainly used in defense field. Anonymous Communication is the main issue in case of MANETs.

2. METHODOLGY

TRUST MANAGEMENT SYSTEM USING SATEM

Service Aware Trusted Execution Monitor (SATEM) is a trusted computing system that achieves trusted code execution of services. A trusted execution monitor in the operating system kernel of the service provider platform, and a trust evaluator on the service requester platform. For peer-to-peer systems, each network node is both the service provider and requester and thereby, has all components. The trusted execution monitor on the service provider sends a commitment to the service requester, which describes all the code files. The service may execute in all circumstances, such as executables, libraries, etc.

It use Dempster-Shafer Theory (DST) which combine separate pieces of observations (evidences) to calculate the probability of malicious behaviors. The basics concept of DST are lack of evidence can not be viewed as the refutal to this evidence. and some solution can be done. A node can either hold a positive opinion or have no opinion to the misbehavior of its neighbor No opinion is called “Environment”.

Advantage

- In this system, user will avoid trusting the vulnerable code.
- Satem kernel code is not modularized attributable to the necessity of inserting integrity check points at numerous places within the kernel. This makes the code troublesome to port and modify. since it provides two-tier security in strong.

Network Formation

Networks are formed with the given range of the sensors. Nodes are grouped automatically depends upon their radio waves Agents are formed for group registration.

Behavioral Data collection

The behavioral data collection module is responsible for the collection of node behaviors and formation of behavioral dataset. To observe the performance of SATEM as well as that of Trust in the following four scenarios: different number of nodes, different radio ranges, different percentage of misbehaving nodes, different node motion speeds.

Node Classification

More specifically, rank is used in experiments to determine the trustworthiness of nodes in a ranked list. Each node observes and records neighbor behaviors, and these local observations are fed into the rank classifier to produce the initial trustworthiness in a ranked list.

Calculate Node Trust

SATEM is used to evaluate the trustworthiness of nodes in MANETs.The local observations and foreign observations obtained from other nodes are fused together using Dempster-Shafer Theory and thus an updated behavioral dataset is generated depends upon the rank list value. If the updated behavioral dataset makes rank classifier produce a ranked list with different order than the previous one, then the updated behavioral dataset is propagated to all neighbors.

Analysis

Analyze the node behavior over the total amount of packets that the node has received such as packet drop rate (PDR), packet modification rate (PMR) and RTS flooding rate. In classification phase, analyze the node density, Radio Range, Adversary percentage, node mobility for calculating the node trust value.

SATEM USING DEMPSTER'S RULE

Node behaviors are identified using Dempster-Shafer Theory and thus an updated behavioral dataset is generated.A kernel based SATEM uses a fixed formula to calculate the trustworthiness of mobile nodes in an automated manner.

The Dempster-Shafer Theory (DST) is used to combine separate pieces of observations (evidences) to calculate the probability of malicious behaviors. The basics concept of DST are lack of evidence can not be viewed as the refutal to this evidence.and some solution can be done. A node can either hold a positive opinion or have no opinion to the misbehavior of its neighbor No opinion is called "Environment".

Dempster's Rule of combination:

The reports from different nodes by applying the Dempster'srule, which is defined as following.

$$m_B(A) \oplus m_C(A) = \frac{\sum_{q,r:\alpha_q \cap \alpha_r = A} m_B(\alpha_q) m_C(\alpha_r)}{1 - \sum_{q,r:\alpha_q \cap \alpha_r = \Phi} m_B(\alpha_q) m_C(\alpha_r)}$$

($m_B \oplus m_C$) A-mass function of evidence(A), which a result of a combination of evidence(B) and evidence(C), k-mass of conflict, $\oplus$- operator direct sum

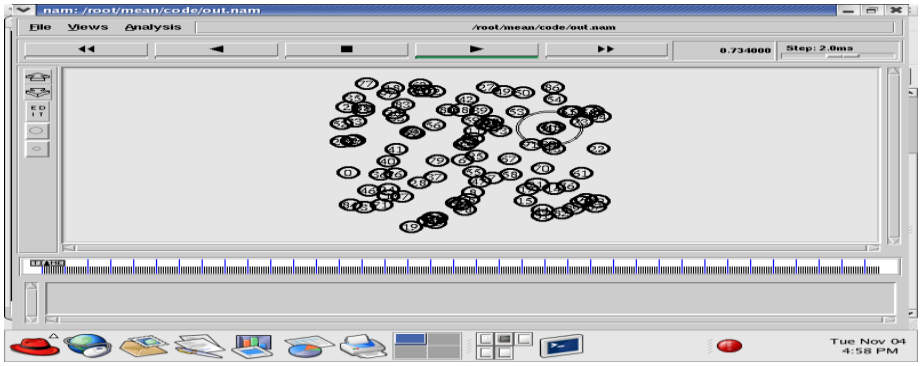
Here m_B (A) denotes the view of node k on another node A

α e - are all the basic events that compose the event α i

3 .EXPERIMENTS AND RESULTS

NETWORK FORMATION

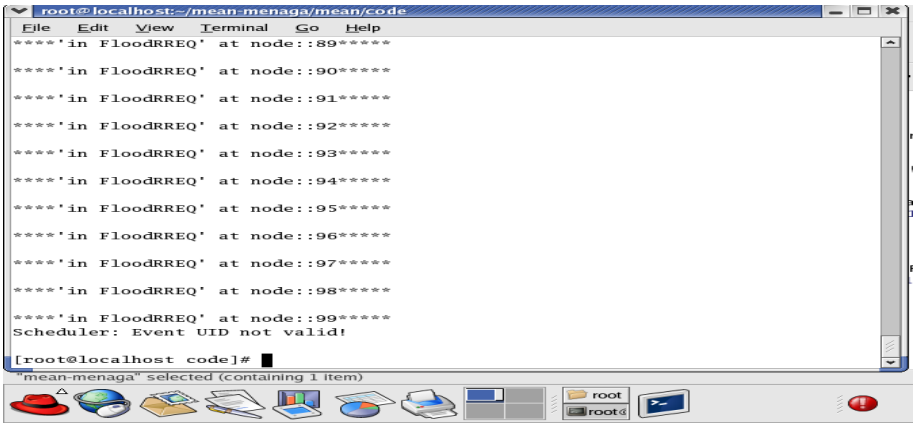
Networks are formed using NS2 simulation tool and flatgrids are created and nodes are created within the given X,Y position. Nodes are placed randomly in a network and communication is performed. TCP & UDP Protocol is used for communication. FTP and CBR traffic is used for file transmission. In this network an attacker model sends the wrong route request and it can be found by the trusted agent node.



Network Formation

ATTACKER NODE SENDS THE FLOOD RREQ

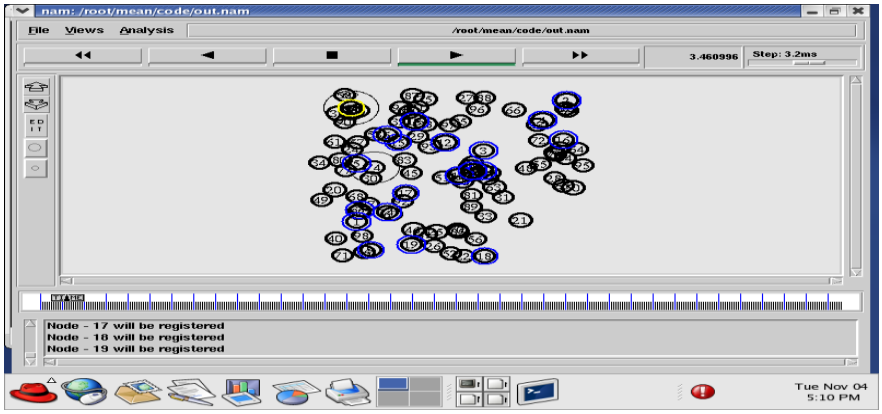
An Attacker model try to connect the network and it sends the Flood RREQ to all the nodes contained in the wireless Network. That is it sends the wrong route request to all the nodes. But it cant connect to the network since an event scheduler identifies this is the wrong user id(UID) as shown in the following figure.



Attacker Node Sends The Flood RREQ

NODES REGISTERATION

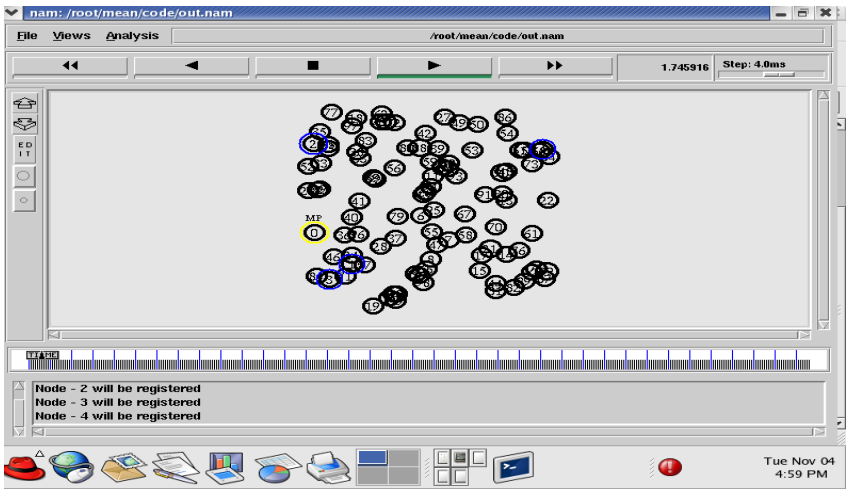
The following Network Animator Window shows that the all nodes are registered for communication. When the node request to communicate first it should registered. After registering it can be communicated and its reports are received by the MP Agent node.



Nodes Registration

NODES CALCULATION

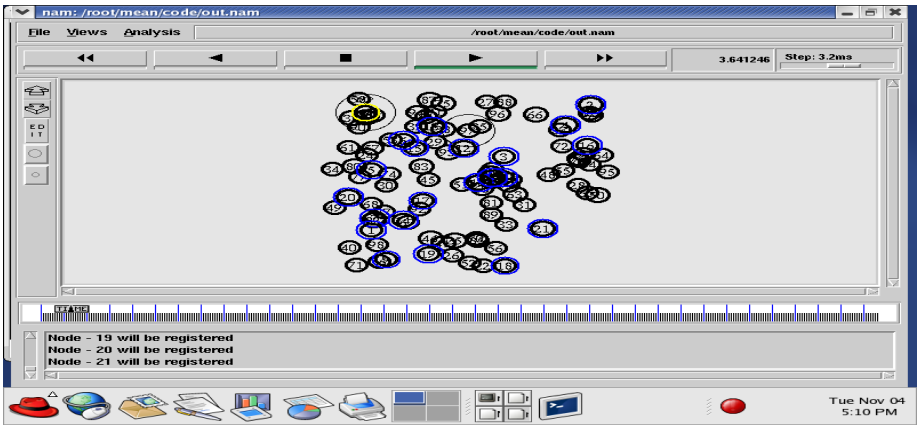
Above Network Animator Window shows that all the nodes are requested and the requested nodes are registered and nodes are evaluated during the transmission by the MP trusted agent node. Since Nodes trust value is calculated by its behavior analysis.



Node Calculation

TRUSTED AGENT NODE INDICATION

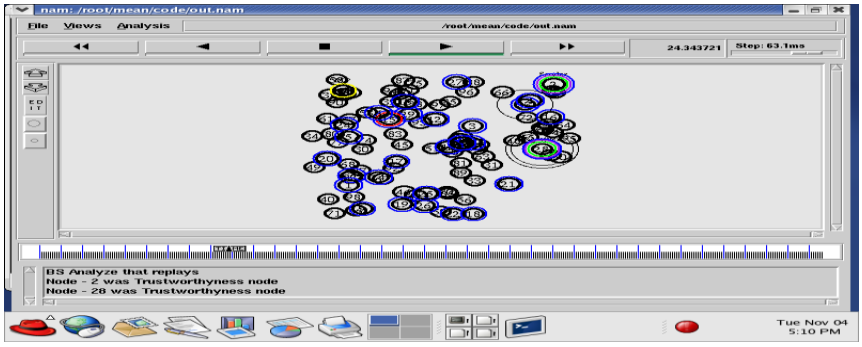
This Network Animator Window shows that the trusted agent node indicated in Yellow color evaluate all the node which are registered. Node evaluation is calculated by its behavior. All the registered nodes are indicated in blue color.



Trusted Agent Node Indication

TRUSTWORTHINESS NODE FOR CONFORMATION

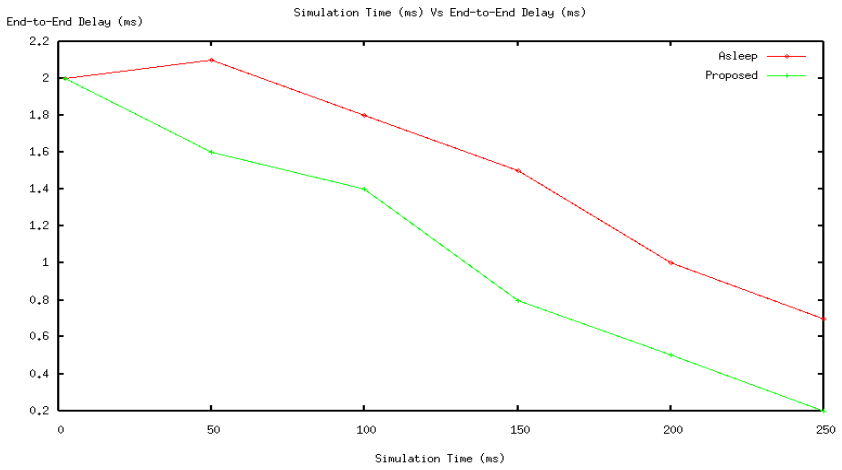
This Network Animator Window shows that the node 2 & 28 wants to communicate and that the two nodes are registered and it will be analyzed by base station and conformation of trust worthiness is displayed and start to communicate.



Trust Worthiness Node For Conformation

SIMULATION RUN TIME VS DELAY

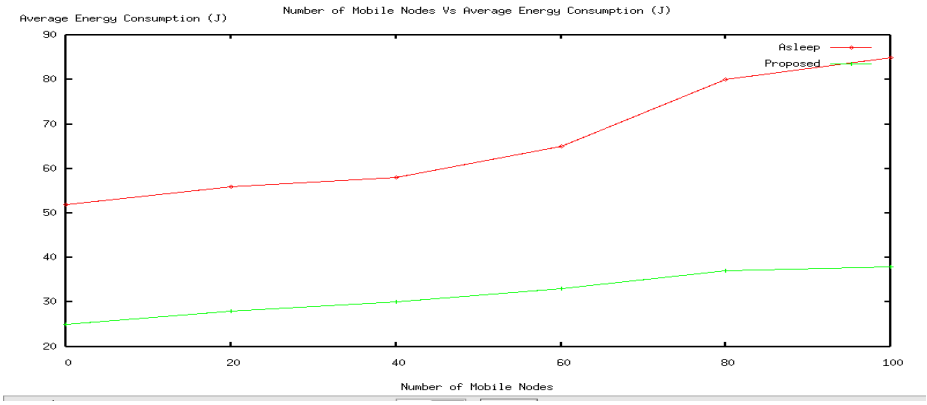
This graph represents comparison of end to end delay of Asleep Routing scheme and Proposed scheme. Performance results shows that the proposed delay time is reduced significantly than the existing system.



Simulation Run Time Vs Delay

MOBILE NODES VS AVERAGE ENERGY CONSUMPTION

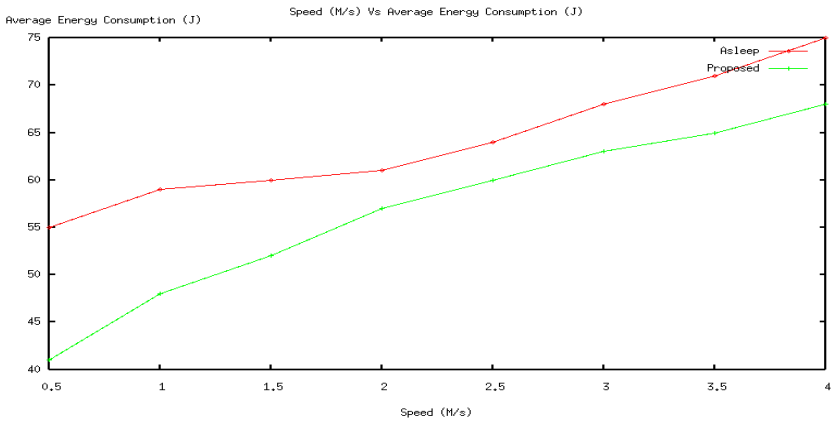
This graph represent Mobile nodes Vs Average Energy Consumption compared with thte existing and proposed system.Performance results of this graph shows that the energy consumption level is very low when compared with the existing system.



Mobile Nodes Vs Average Energy Consumption

SPEED VS AVERAGE ENERGY CONSUMPTION

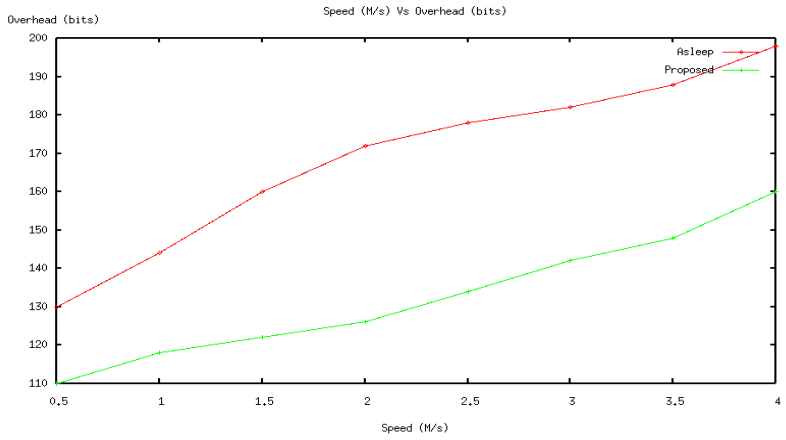
This graph shows that the speed with Energy Consumption is compared with the existing and proposed system. Performance results of the proposed system is in decreased range when the speed was increased in range.



Speed Vs Average Energy Consumption

SPEED VS OVERHEAD

This graph shows Nodes response in terms of speed with their overhead is compared with the existing and proposed system.Performance of the proposed system results decreased when the speed and its overhead was increased.



Speed Vs Overhead

4. CONCLUSION AND FUTURE ENHANCEMENT

The purpose of trust management schemes is to properly evaluate the trustworthiness of nodes and thus identify and mitigate misbehaviors. A Flooding RREQ(Route request) of attacker is identified by its wrong scheduler event user id and prevent them in an effective way by using the scheme SATEM. The SATEM scheme is for automatic machine learning to classify nodes by its behavioursand identifies whether the nodes as malicious or not and it uses DST which combine separate pieces of observations (evidences) to calculate the probability of malicious behaviors.

In the proposed system flooding attacks is prevented and SATEM, Dempster-Shaper Theory is used to evaluate the node behavior and its trustworthiness. In future analyze the Reduction of Quality attacks, is a milder form of the DOS attacks but these are more difficult to detect than the traditional flooding attacks. The goal of these attacks do-not wish to completely cut-off services and resources or damage resources, instead only wish to reduce the QoS offered to the users of the systems and the services of the system.In future plan is to implement a flow monitoring technique is proposed to mitigate the impact of ROQ attacks in wireless networks.

REFERENCES

[1] M. Carvalho, "Security in mobile ad hoc networks," *IEEE Security Privacy*, vol. 6, no. 2, pp. 72–75, Mar. 2008.

[2] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 1, pp. 188–190, July 2013.

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 38–47, Feb. 2004.

[4] Q. Guan, F. R. Yu, S. Jiang, and V. Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2674– 2685, July 2012.

[5] J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 806–815, Feb. 2009.

[6] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3064–3073, Sept. 2011.

[7] Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," in *Proc. 2000 ACM MOBICOM*, pp. 275–283.

[8] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 48–60, Feb. 2004.

[9] T. Alpcan and T. Basar, *Network Security: A Decision and Game Theoretic Approach*. Cambridge University Press, 2010.

[10] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 472–486, 2013.

