International Journal of Computational Intelligence and Informatics, Vol. 2: No. 1, April - June 2012

Smart Way for Secured Communication in Mobile Ad-hoc Networks

P. Infant Kingsly
CSE Department, R.M.K Engineering College
Anna University Affiliated
Chennai, India
infantkingsly@gmail.com

C. Jayakumar
CSE Department, R.M.K Engineering College
Anna University Affiliated
Chennai, India
cjk.cse@rmkec.ac.in

Mahendran Sadhasivam
CSE Department, R.M.K Engineering College
Anna University Affiliated
Chennai, India
mahent11@gmail.com

S. Deepan Chakravarthy
CSE Department, R.M.K Engineering College
Anna University Affiliated
Chennai, India
sdcdeepan@gmail.com

***Abstract*— The application of multi-modal biometric methods in securing mobile ad-hoc network has been addressed in this paper. A MANET is an infra structure less network for mobile devices connected by wireless link. The mobile network is often vulnerable to security attacks even though there are many traditional approaches, due to its features of open medium and dynamic changing topology. Multi-modal biometrics is deployed to work with intrusion detection systems (IDSs) to overcome the shortcomings of uni-modal biometric systems. The cluster head is elected in which Dempster-Shafer theory is evaluated in order to increase the observation accuracy to maintain high security and trusted MANET. Since each device in the network has measurement and estimated limitations, more than one device needs to be chosen, and observations can be fused to increase observation accuracy using Dempster–Shafer theory for data fusion.**

Keywords — MANET- Mobile Adhoc Network, IDS- Intrusion Detection System, ANN- Artificial Neural Network, DT – Decision Tree.

I. INTRODUCTION

The mobile ad-hoc networks (MANET) are becoming more attractive for use in military applications. The MANETs are the recent advances in mobile computing and wireless communication. Supporting security – sensitive application in hostile environment has become an important research area for MANETs [8]. A MANET is a self-configuring infra structure less network of mobile devices connected by wireless link. Due to this mobile network is often vulnerable to security attacks. 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. In high security MANETs, user authentication is critical in preventing unauthorized user from accessing or modifying network resources. Hence in MANET authentication is done continuously and frequently [1]. User authentication can be performed by using one or more types of validation factors: knowledge factors, possession factors, and biometric factors. Knowledge factors (such as passwords) and possession factors (such as tokens) are very easy to implement but can make it difficult to distinguish an authentic user from an impostor if there is no direct connection between a user and a password or a token. Biometrics technology, such as the recognition of fingerprints, irises, faces, retinas, etc., provides possible solutions to the authentication problem [5]. In addition, intrusion detection

systems (IDSs) are important in MANETs to effectively identify malicious activities and so that the MANET may appropriately respond. IDSs can be categorized as follows 1) network-based intrusion detection, which runs at the gateway of a network and examines all incoming packets; 2) router-based intrusion detection, which is installed on the routers to prevent intruders from entering the network; and 3) host-based intrusion detection, which receives the necessary audit data from the host's operating system and analyzes the generated events to keep the local node secure. For MANETs, host-based IDSs are suitable since no centralized gateway or router exists in the network [7].

II. RELATED WORKS

Certificate Authorities (CA) for authentication in ad hoc mobile networks and proposed a method with multiple certificate authorities CAs based on threshold cryptography [2]. These multiple CAs have secret shares of a Certificate Authority Signing Key (CASK) while no CAs individually know the whole complete CASK, which can be known only when CAs of more than M nodes collaborate. An attacker has to break into a threshold number of servers in order to get access to the secret key of the service. To prevent compromises of the server, share refreshing is periodically done. This approach has some weaknesses for example nodes that are designated to be servers have to work more than others. It is also difficult for the servers to know the Public keys of all the nodes in an ad hoc mobile network especially if it is large. In popular network authentication architectures, two entities authenticate each other via certificates issued by a trusted certification authority (CA).

The fully-distributed certificate authority extends the idea of the partially-distributed approach by distributing the certificate services to every node [2]. In this approach, after the bootstrapping phase, a new node can join the network at anytime through self-initialization. This node can obtain its own secret share of CASK with the help of M local neighbor nodes. Although this approach enhances scalability and availability, it still depends on an offline authority during the bootstrapping phase.

Narasimha [2] pointed out the weakness with Luos' authentication approach that is the secret sharing, based on RSA signature does not provide an important property known as verifiability. They proposed the method for group admission control in peer-to-peer systems which are given a trustable CA. It is based on DSA signature which has verifiability.

Hubaux [2] proposed a scheme based on a chain of Public-key certificates, which is scalable and self-organized. Their approach involves issuing certificates by the users themselves without the involvement of any certificate authority.

Capkun [2] proposed an authentication method and asserted that, mobility helps security. Their key idea was that, if two nodes are in the vicinity of each other, they can establish a security association (SA) by exchanging appropriate cryptography materials through a secure channel with short transmission range.

Seongil [2] pointed out that, this direct solution takes a long time because it requires a node to encounter every node that it wants to communicate with. As years go both security issues and authentication methods are improving along the growth of MANET [2]

III. EXISTING SYSTEM

A. Uni-modal biometric approach

The various components of the networks are sensor (capable of distributing information), node or host. The individual sensor is responsible for validating the user request and respond instantly by the same sensor. The level of observation is minimum. The entire system is working in trust worthy basis node may not be aware of sensor state it blindly accept the result produced by the sensor. The two states of the sensors are (1) secure and (2) compromised. During the compromised state sensor will never validate and accept the node blindly. This may results in security breaches.

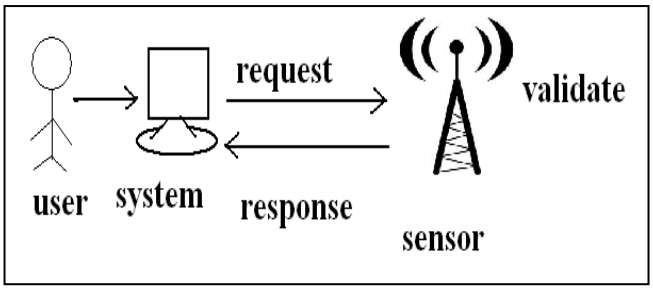

Figure 1 Uni-Modal Approach

IV. PROPOSED SYSTEM

A. Multi-modal biometric approach

Distributed combined authentication and intrusion detection with data fusion [7] [4] in mobile ad-hoc networks (MANETs). Multi-modal biometrics [8] is deployed to work with intrusion detection systems (IDSs) [7] to alleviate the shortcomings of uni-modal biometric systems. Since each device in the network has measurement and estimation errors, more than one device needs to be chosen, and observations can be fused to increase observation accuracy using Dempster-Shafer theory [7] [3] for data fusion. The system decides whether or not user authentication (or IDS input) is required, and which biosensors (or IDSs) should be chosen depending on the security posture. The decisions are made in a fully distributed manner by each authentication device and each IDS [7].

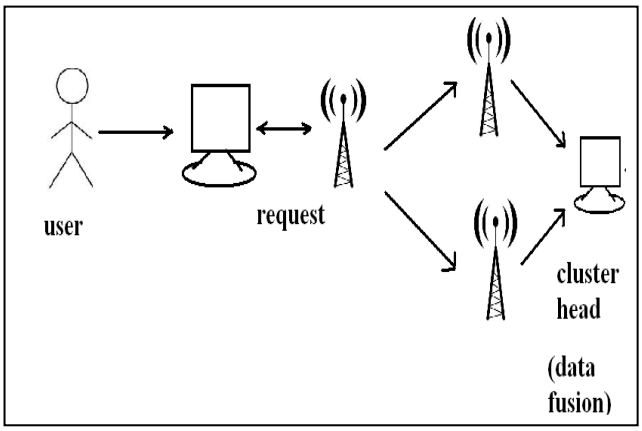

Figure 2 Multi- Modal Approach

V. METHODOLOGY USED IN HIGH SECURITY MANET

A. *Biometric Systems* include two kinds of system modals

- Identification.
- Authentication.

The proposed system operates in authentication mode. It works based on a comparison of the matching score between the input sample and the enrolled template within each and every host with a decision threshold, each biometric system outputs a binary decision: accept or reject.

B. Intrusion Detection System

Two main techniques

- Misuse detection
- Anomaly based detection

Multiple algorithms have been applied to model attack signature or normal behavior patterns of systems [7] [1].

Three common algorithms are described in the next subsections

i) Decision tree (DT)

- DT is a useful machine learning technique, is used to organize the attack signatures into a tree structure [6].
- A DT takes an object (or) situation described by a set of attributes and returns the predicted output values for the input (i.e.) "decision".

ii) Artificial neural networks (ANN)

The ANNs are very different from expert systems since they do not need a knowledge base to work. Instead, they have to be trained with numerous actual cases. An ANN is a set of elementary neurons which are connected together in different architectures organized in layers what is biologically inspired [6].

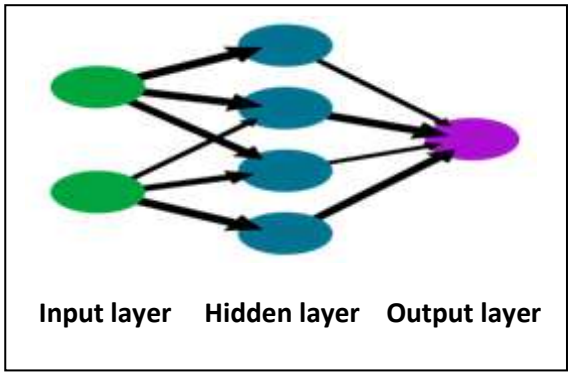

Figure 3 Neural Networks

The Figure 3 shows the feed forward artificial neural network architecture for pattern recognizing based on the given input provided by user.

iii) Naive bayes

A naïve bayes classifier is based on a probabilistic model to assign the most likely class to a given instance [6]. The naive Bayes probabilistic model abstractly, the probability model for a classifier is a conditional model

$$P\left(C \mid F_1, \ldots\ldots, F_n\right) \quad (1)$$

over a dependent class variable *C* with a small number of outcomes or *classes*, conditional on several feature variables F_1 through F_n which is shown in (1). The problem is that if the number of features *n* is large or when a feature can take on a large number of values, then basing such a model on probability tables is infeasible. We therefore reformulate the model to make it more tractable.

Using Bayes' theorem, we can write the equation as in (2).

$$P(C \mid F_1, ..., F_n) = \frac{P(C)P(F_1, ..., F_n \mid C)}{P(F_1, ..., F_n)} \quad (2)$$

C. Data Fusion

In proposed scheme L sensors are chosen for authenticating and intrusion detection at each time slot to observe the security state of the network

- To obtain the security state of the network, these observation values are combined and decision about the security state is made.
- Sensor might be in either the state (1) secure and (2) compromised.
- If so sensor in compromised state they may results in inaccurate assessment. It's quite difficult to ascertain which observers are compromised.

Therefore, choosing an appropriate fusion method is critical in our proposed scheme we use DEMPSTER SHAFER THEORY [7] [3] for measuring probability of the secured state of sensor node.

VI. SYSTEM MODEL

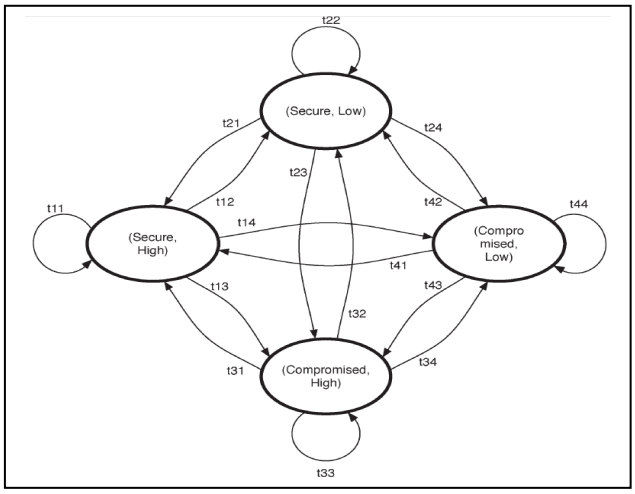

Figure 4 Example of markov chain for a single node's state transition

Figure 4 Shows transition diagram for sensor states using markov chain model Security states of the sensor are (1) Secure and (2) compromised Energy state of the sensors are (1) High and (2) low. These are various probability of state transition.

VII. SIMULATION RESULTS

In this section, we use computer simulations to evaluate the performance of the proposed scheme with and without using data fusion. We consider the following simulation scenario: A MANET is equipped with two biosensors for continuous authentication, iris sensor, and fingerprint sensor. Each sensor Includes two security states, i.e., safe and compromised, and two energy states, i.e., high and low, which means that there are four states for each sensor. The iris sensor is more expensive and also provides more accurate authentication. The

fingerprint sensor provides intermediate security authentication and has intermediate energy cost. There is an IDS in the MANET, which uses the least energy and has the least accuracy in detecting the security state.

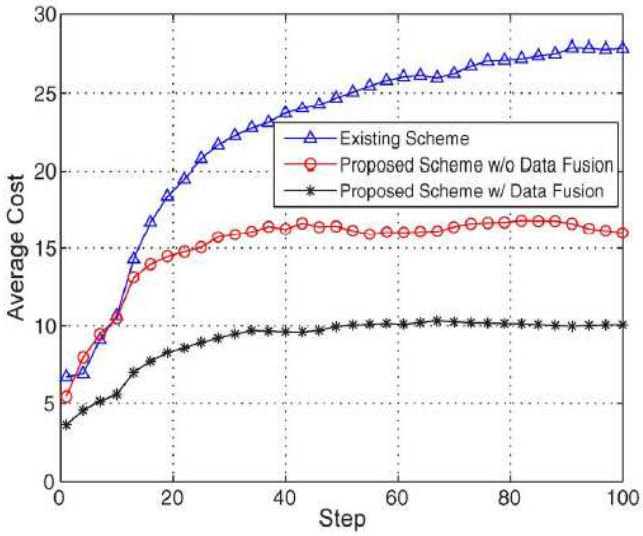

Figure 5 Cost comparisons among the proposed scheme with data fusion, the proposed scheme without data fusion, and the existing scheme

Figure 5 shows the cost estimation is done between existing and proposed scheme (with and without data fusion). The cost and network traffic are directly proportional. In existing system, there are many possibilities of intruder to increases the network traffic. Thus the simulation result predict that cost increases exponentially in powers of 2(twice) when compared to the proposed system. The cost is decreased by 5% with each and every advancement in the scheme.

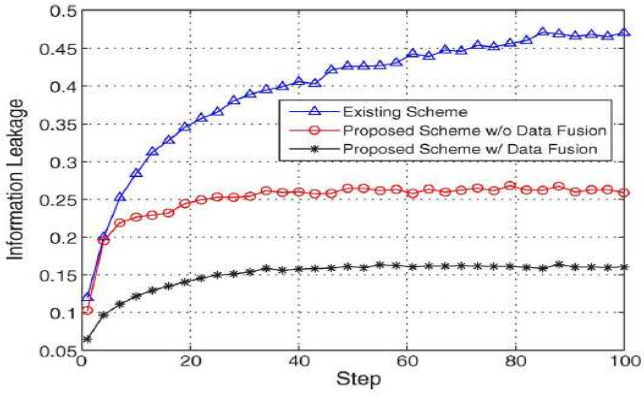

Figure 6 Information leakage comparisons among three schemes.

Figure 6 shows the leakage of information to the un-trusted node in both existing and proposed scheme. Due to the less observation the probability of intruder is high in the existing system. The simulation results at 20th step the proportion of information leakage is 0.35(bytes) in existing system and 0.15-0.25(bytes) in proposed system. The percentage difference is (10-15%) with each and every scheme.

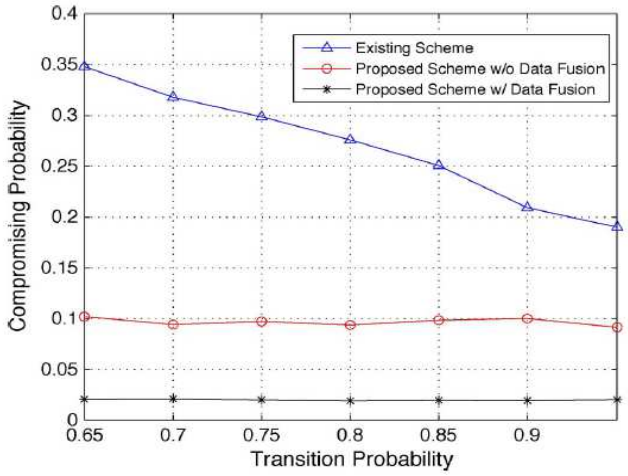

Figure 7 Network compromise comparisons among three schemes under different transition probabilities

Figure 7 shows the compromising probability between uni-modal and multi-modal approach. Due to the estimated limitations of biosensors it needs to choose more number of sensors to validate. Since in uni-modal approach one sensor is responsible for authenticating the user the probability of sensor is high. The simulation result at a instant is 0.35 for existing system where as for proposed system is 0.1 probability. There will be a steep change from existing and proposed scheme in compromising the network.

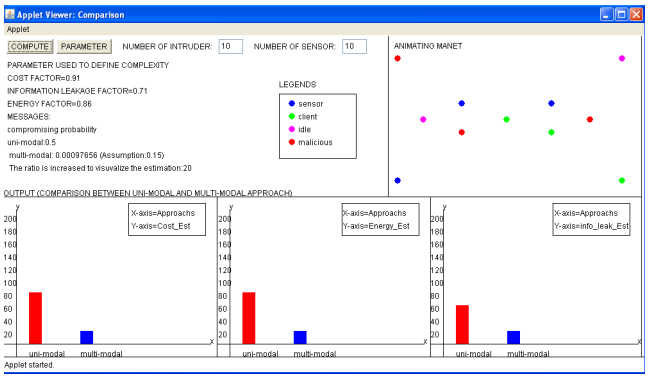

Figure 8 comparing the existing and proposed scheme based on the number of intruder and number sensor

Figure 8 simulations to define the complexity and to compare with the existing system. The three different factors are used to estimate cost, energy spend and information leakage with their fixed compromising probability.

VIII. CONCLUSION AND FUTURE WORK

Combining continuous authentication and intrusion detection can be an effective approach to improve the security performance in high-security MANETs [7] [5]. In this paper, we have presented a distributed scheme combining authentication and intrusion detection. In the proposed scheme, the most suitable biosensors for authentication or IDSs are dynamically selected based on the current security posture and energy states. To improve upon this concept, Dempster–Shafer theory has been used for IDS and sensor fusion since more than one device is used at each time slot [7] [3]. The distributed multi-modal biometrics and IDS scheduling process can be divided into offline and online parts to mitigate the computational complexity [8].

Further work is in progress to reduce the computation complexity of the proposed scheme by searching for some structured solutions to the distributed scheduling problem. In addition, we plan to consider more nodes' states, such as mobility and wireless channels, in making the scheduling decisions in MANETs.

ACKNOWLEDGMENT

We convey our thanks to our chairman R.S.Munirathinam and vice-chairman R.M.Kishore who took keen interest on us and encouraged throughout the course of study and for their kind attention and valuable suggestions offered to us throughout the course of study.

We express our sincere thanks to our director R.Jothi Naidu and principal Elvin Chandra Monie for their whole hearted and kind co-operation.

We are highly thankful to our head of the department professor K.L.Shunmuganathan for rendering us all facilities for undertaking the projects. We are also thankful to our internal guide professor C.Jayakumar for his extended support and guidance in the successful outcome of this project.

We extend our thanks to all the faculties of the department of Computer Science and Engineering, who were behind us throughout the course of study.

REFERENCES

[1] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos, National Institute of Standards and Technology "Detecting Critical Nodes for MANET Intrusion Detection Systems" Proceedings of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (2006).

[2] Godfrey onyait-omoda, Makerere University, "A Framework for Improving Network Security in Ad Hoc Mobile Networks" February, 2006.

[3] Huadong Wu1, Mel Siegel, Rainer Stiefelhagen, JieYang, Robotics Institute, Carnegie Mellon University "Sensor Fusion Using Dempster-Shafer Theory" IEEE Instrumentation and Measurement Technology Conference Anchorage, AK, USA, 21-23 May 2002.

[4] Jie Liu, F. Richard Yu, *Senior Member, IEEE,* Chung-Horng Lung, and Helen Tang, "Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks", IEEE transactions on wireless communications, vol. 8, no. 2, February 2009.

[5] Sheng Zhang, Rajkumar Janakiraman, Terence Sim, and Sandeep Kumar "Continuous Verification Using Multi-modal Biometrics" School of Computing, National University of Singapore, ICB 2006.

[6]Stuart Russell and Peter Norvig "Artificial Intelligence A Modern Approach", 2nd edition Pearson Education publication 2009.

[7**]** Thomas M. Chen and Varadharajan Venkataramanan Southern Methodist University, "Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks" In IEEE Internet Computing Published by the IEEE Computer Society NOVEMBER DECEMBER 2005.

[8] Q. Xiao, "A biometric authentication approach for high security mobile adhoc networks" In Proceeding IEEE Information Assurance Workshop, West Point, NY, June 2004.