ISSN:0975-9646

J.Deny et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5) , 2011, 2213-2215

Implementation of High Security in MANET Using Combined IDS and Finger Print Authentication with Data Fusion

J. Deny and N. Sivasankari

Dept. of Electronics & Communication Engg.,
Kalasalingam University, Krishnankoil, Srivilliputtur, India.

***Abstract*— This paper is an attempt to study and implement high security in Mobile Ad-hoc Networks (MANETs) using Multi-modal biometric technology and by using Dempster-Shafer theory for data fusion. MANETs supporting security-sensitive applications in hostile environments needs to be continuously monitored for unauthorized use. In such cases, continuous verification is needed. In this paper we study and present the theory, architecture, implementation and performance of a multimodal combined IDS and Finger print authentication with data fusion providing authentication in a distributed manner.**

***Keywords*— Multimodal biometric, MANET, Data Fusion, IDS, Dempster-Shafer Theory.**

I. INTRODUCTION

Wireless nodes can establish a dynamic network without the need of a fixed infrastructure. This type of network is very useful in tactical operations where there is no communication infrastructure. Due to rapid development in self-configuration and self-maintenance capabilities, Mobile Ad-Hoc Networks (MANETs) have become a popular subject. In recent years, MANETs are becoming popular in security-sensitive applications in hostile environments like military applications. Mobility and high-speed access to voice and data communication links are highly desirable in military environments. Military organizations depend on secure and reliable communication systems in order to strategize, command, control, and operate their forces in their respective environments, in land, sea, or air. Authentication can be considered as the keystone of network security because it is the first step toward prevention of, and guarding against, unauthorized access to network resources and sensitive information. MANETs which are supporting high sensitive applications in hostile environments need to monitor continuously for unauthorized use. This is because; security is a major concern for providing trusted communications in a potentially hostile environment. Two complementary classes of approaches to protect from unauthorized. The two complementary classes of approaches are prevention-based approaches, such as authentication and detection-based approaches, such as intrusion detection. There are more number of ways to provide validation for user authentication. Some of the factors are 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 [2]. Biometrics technology, such as the recognition of fingerprints, irises, faces, retinas, etc. provides possible solutions to the authentication problem [3]. But for high security applications MANETs also need the second class of approach that is detection-based approaches, such as intrusion detection. This is because there are always some weak points in the system, no matter what is used for authentication, so it is more important to provide multi-level protections. Intrusion Detection Systems (IDSs) solves this problem by serving as the second wall of protection, and it can effectively help in identifying malicious activities. An IDS continuously or periodically monitors the current subject activities, compares them with stored normal profiles and/or attack signatures, and initiates proper responses [4]. Authentication is an important type of responses initiated by an IDS. After an authentication process, only authentic users can continue using the network resources and compromised users will be excluded [5].

Biometrics provides some possible solutions to authentication used in MANETs since it has the direct connection with user identity and needs little user interruption. Each biometric technology has its own strengths and weaknesses. Currently, there is no best biometric modality since it depends on the environment applied. Unimodal biometrics has to face several challenges such as noise in sensed data, intra-class variations, inter-class similarities, and etc. Some of these problems could be resolved by adopting multimodal biometric systems. Multimodal biometric system presents a more reliable authentication method due to the combination of statistically independent biometric traits [6]. This system can exploit the benefits of one biometric and mitigate the shortcomings.

II. RELATED WORKS

As the front line of defense, user authentication is crucial for integrity, confidentiality and non-repudiation. Biometrics has a direct connection with the identity of the user, and has been studied in MANETs

T. Sim et. al. [6] proposed a continuous biometric based authentication. The System was a multimodal biometrics verification system which continuously verifies the presence of a logged-in user. The proposed system [6] imposed additional requirements on multimodal fusion when compared to conventional verification systems. The system was also sufficient for high-security environments

in which the protected resources needs to be continuously monitored for unauthorized use.

J. Koreman et. al. [7], addressed the biometric-based continuous authentication system. [7] proposed multimodal biometric authentication based SecurePhone mobile communication system. This system gave access to e-signing, m-contracts in a secured authenticated approach. Based on several test using fusion techniques for biometric evidence combination, an efficient multi-modal biometric authentication was achieved on the SecurePhone PDA.

Altinok et. al. [8] proposed a multimodal system that performed authentication continuously by integrating information temporally as well as across modalities. The proposed modal [8] has also another advantage of providing ongoing verification and can easily be coupled with another system for dynamically adjusting access to privileges accordingly. The system operates continuously by computing expected values as a function of time differences. The temporal integration method depends on the availability of past observations.

J. Muncaster et. al. [9] addressed the issue of post-login user verification using multimodal approach of dynamic Bayesian networks. The proposed framework [9] monitors the characteristics of the user throughout the session in order to provide continuous verification of identity. Another main advantage of the system is the system can also be extended to incorporate important contextual information. Test were performed using face recognition and keystroke dynamic and results shown a promise and warrant future work to develop a more controlled experiments for use of additional modalities to improve the robustness of the system.

Xiaofeng Zhao et. al. [10] introduced a data fusion-based intrusion detection model. The intrusion detection problem was converted into an abstracting process that abstracts the system's information from the low-level to high-level; further more points out that different basic detector's output should be fully fused in order to get the detection more accurate. [10] also introduced the evidence theory to the information layer of the model.

Motivated by the results of [6], [7], [8], [9] and [10], we propose a fully distributed scheme of combining intrusion detection and continuous authentication in MANETs.

III. DEMPSTER-SHAFER'S THEORY FOR DATA FUSION

The Dempster-Shafer's framework is a formal framework for combining sources of evidence, it is originally developed by Dempster and extended by Shafer [11]. Its main difference to probability theory, which **is** treated as a special case, is that it allows the explicit representation of ignorance and combination of evidence. This explicit representation of ignorance, or the impression of evidence, makes the use of the D-S theory particularly attractive for complex systems. The combination of evidence is expressed by Dempster's combination rule, which allows the expression of aggregation of necessary in a model using sources of evidence. The D-S framework is based on the view that proposition can he regarded as subsets of a given set of hypotheses. For example, in the intrusion detection system, we can regard the set of hypotheses as the set of categories of infusion. Each anomalous event, then, is a subset of **Ω**. Thus, the propositions of interest are in a one-to-one correspondence with the subsets of **Ω** , and the set of all propositions corresponds to the set of all subset of **Ω** , which is denoted 2^{Ω} . **Ω** is named a frame ***of*** discernment, and the proposition are said to be discemed by the frame [12], [13], [14].

In the process of applying D-S in IDS, firstly, each agent (sensor) collects information in its respective domain, and then the identification of some proposition is generated, which serves as evidence in D-S. Based on these, the BPAF **is** formulated to assign the confidence degree on each proposition. As a BPAF and its corresponding frame of discernment are called a body of evidence, each sensor therefore corresponds to a body of evidence. The essence of multi-sensor data fusion is that within the same frame of discernment, different bodies of evidence, depending on fusion rules, are fused into a resultant BPAF, on which system makes final decision based on decision rules.

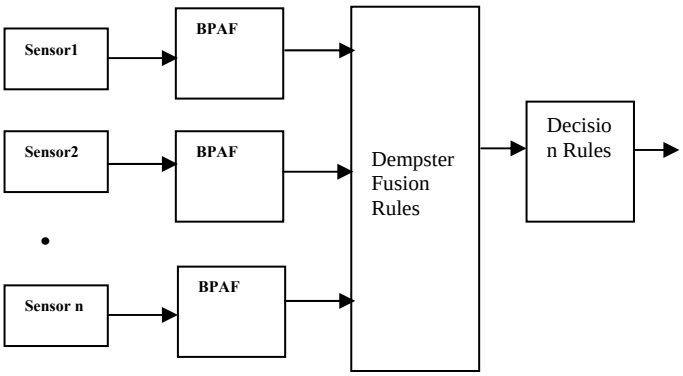


Figure 1: Architecture

IV. SIMULATION RESULTS AND DISCUSSIONS

In this section, we use computer simulations to evaluate the performance of the proposed scheme with and without using data fusion. The simulation scenario involves a device used by a soldier who can use fingerprint biosensor or iris biosensor for user-to device authentication. We consider a two-state HMM problem with two biosensors: one is iris biosensor, the other one means no biosensor will be used, and we estimate the system state using HMM state predictor. Here we call it prediction biosensor.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.

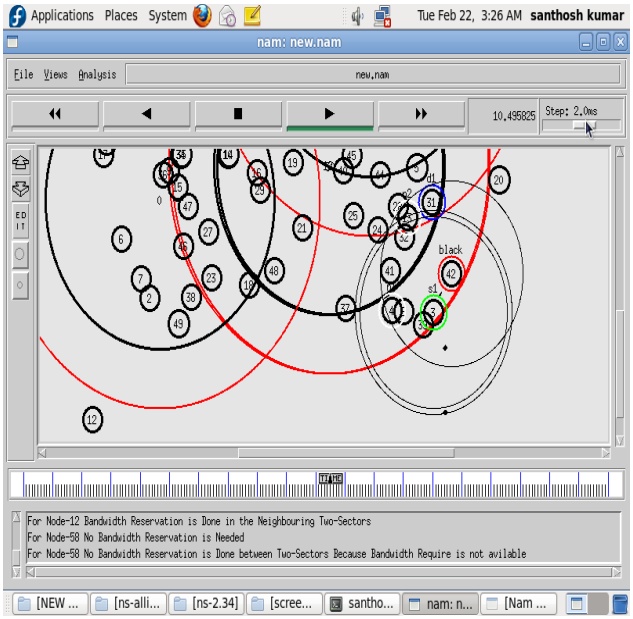


Figure 2: NS2 Implementation Snapshoot

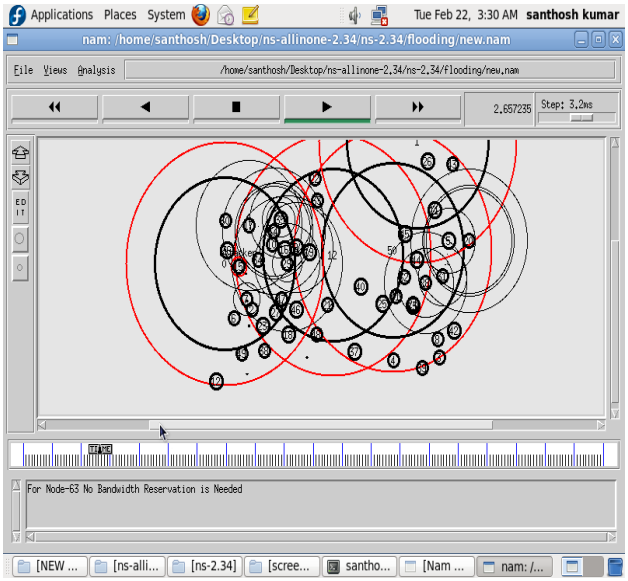
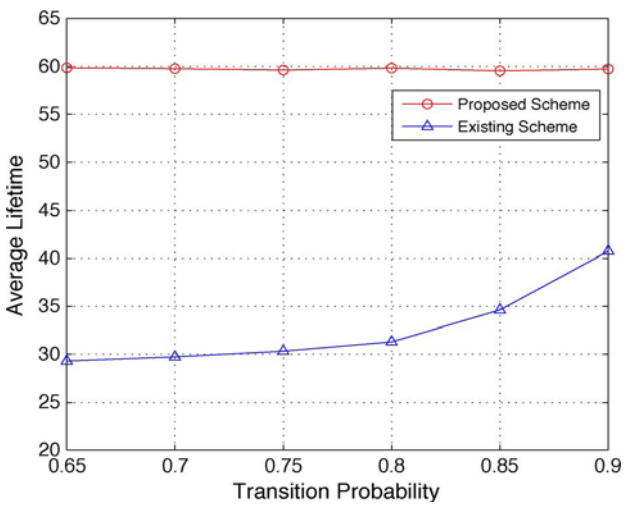


Figure 3: NS2- Implementation Snapshoot



V. CONCLUSIONS

One-time authentication is inadequate for MANETs, especially in some tactical environments. Extra requirements such as little resources consumed for authentication schemes are necessary since there is no fixed infrastructure available in MANETs. Multimodal biometrics provides the possibility to meet all the requirements of authentication in MANETs. MANETs are important to the military for their quick setup, takedown, and mobility features. In securing these networks, authentication is identified as the first line of defense. In tactical operations which require secure MANETs, authentication is a challenge without a central authority. In this paper, we presented the authentication schemes for MANETs from the perspective of a military scenario. Combining continuous authentication and intrusion detection can be an effective approach to improve the security performance in high-security MANETs. In this paper, we have proposed a novel framework to combine intrusion detection and continuous authentication in high security MANETs. Intrusion detection is modeled as noisy sensors that can detect the system security state (safe or compromised). Continuous authentication is performed with multimodal biometrics.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. The problem has been formulated as a POMDP multiarmed bandit problem, and its optimal policy can be chosen using Gittins indexes. The distributed multimodal biometrics and IDS scheduling process can be divided into offline and online parts to mitigate the computational complexity. Simulation results have been presented to show that the proposed scheme can improve network security.

REFERENCES

[1] M. Castro, M. Costa, and A. Rowstron, “Performance and dependability of structured peer-to-peer overlays,” in *Proc. DSN*, Jun. 2004, pp. 9–18..

[2] J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[3] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, “A novel ultrathin elevated channel low-temperature poly-Si TFT,” *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[4] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, “High resolution fiber distributed measurements with coherent OFDR,” in *Proc. ECOC’00*, 2000, paper 11.3.4, p. 109.

[5] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, “High-speed digital-to-RF converter,” U.S. Patent 5 668 842, Sept. 16, 1997.

[6] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[7] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/

[8] *FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.

[9] “PDCA12-70 data sheet,” Opto Speed SA, Mezzovico, Switzerland.

[10] A. Karnik, “Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP,” M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[11] J. Padhye, V. Firoiu, and D. Towsley, “A stochastic model of TCP Reno congestion avoidance and control,” Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[12] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.