ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

Highly Secure Distributed Authentication and Intrusion Detection with DataFusion in MANET

S.Jeyashree

Abstract—**Continuous user-to-device authentication is a challenging task in high security mobile adhoc networks (MANETs). This paper provides distributed combined authentication and intrusion detection with data fusion in such MANETs. Multimodal biometrics are deployed to work with intrusion detection systems (IDSs) to avoid the shortcomings of unimodal biometric systems. Since each device in the network has specific measurement and estimation limitations, more than one device needs to be chosen, and observations can be fused to increase observation accuracy using Dempster–Shafer theory .This theory is used for the accurate observation of the device connected in the internet and in the sensor. The system decides whether 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 IDS.**

Index Terms— **Authentication, biometrics, intrusion detection, mobile ad hoc networks (MANETs), security.**

I. INTRODUCTION

In high-security MANETs, user authentication is critical in preventing unauthorized users from accessing or modifying network resources. Because the chance of a device in a hostile environment being captured is extremely high, authentication needs to be performed continuously and frequently. 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 [4]. 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 [6]: 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. In the framework proposed in [9], multimodal biometrics are used for continuous authentication, and the IDSs are modeled as sensors to detect the system's security state. The framework is shown to be effective as it combines an important prevention-based security approach and a detection-based approach. In this paper, we propose a fully distributed scheme of combining intrusion detection and continuous authentication in MANETs. Several distinct features of the proposed scheme are given here.

1. In the proposed scheme, multimodal biometrics are deployed to alleviate the shortcomings of unimodal biometric systems.

2.Since each device in the network has measurement and estimation limitations, more than one device can be chosen, and their observations can be fused to increase observation accuracy. Dempster–Shafer theory [11] is used for data fusion.

3. The system decides whether a user authentication (or IDS) is required and which biosensors (or IDS) should be chosen, depending on the security posture. The decisions are made in a fully distributed manner by each authentication device and IDS. Since there is no need for a centralized controller, the proposed scheme is more generic and flexible than a centralized scheme in MANETs. Nodes can freely join and leave from the network.

4. Since a biometric authentication process requires a large amount of computation, the energy consumption is significant. Moreover, due to the dynamic wireless channels in MANETs, the energy consumption for data transmissions is dynamically changing Therefore, in the proposed scheme, energy consumptionis also considered to improve the network lifetime.

II. BIOMETRIC-BASED USER AUTHENTICATION:

Biometric technology can be used to automatically and continuously identify or verify individuals by their physiological or behavioral characteristics.

Biometric systems include two kinds of operation models:

1) Identification
2) Authentication.

In the proposed system, the biometric systems operate in authentication mode (one-to-one match process) to address a common security concern: positive verification (the user is whoever the user claims to be). Based on a comparison of the matching score between the input sample and the enrolled template with a decision threshold, each biometric system outputs a binary decision: accept or reject. In most real-world implementations of biometric systems, biometric templates are stored in a location remote to the biometric sensors . In biometric authentication processes, two kinds of errors can be made:

1) false acceptance (FA)
2) false rejection (FR).

FAs result in security breaches since unauthorized persons are admitted to access the system/network. FRs result in convenience problems since genuinely enrolled identities are denied access to the system/network, and maybe some further checks need to be done. The frequency of FA errors and of FR errors are called FA rate (FAR) and FR rate (FRR), respectively. The FAR can be used to measure the security characteristics of the biometric systems since a low FAR implies a low possibility that an intruder is allowed to access the system/network. In tactical MANETs, failure in user authentication might result in serious consequences. Hence, more than one biometric sensor is used at each time period in our system to increase the effectiveness of user authentication.

II. IDSs:

Intrusion detection is a process of monitoring computer networks and systems for violations of security and can be automatically performed by IDSs. Two main technologies of identifying intrusion detection in IDSs are given as follows: misuse detection and anomaly detection. Misuse detection is the most common signature-based technique, where incoming/ outgoing traffic is compared against the possible attack signatures/ patterns stored in a database. If the system matches the data with an attack pattern, the IDS regards it as an attack and then raises an alarm. The main drawback of misuse detection is that it cannot detect new forms of attacks. Anomaly detection is a behavior-based method, which uses statistical analysis to find changes from baseline behavior. This technology is weaker than misuse detection but has the benefit of catching the attacks without signature existence.
In the proposed scheme, a Markov model is used. Let the state of an arbitrary sensor n, $n \in \{1, 2, \ldots, N\}$ be $x_{(n)}(t)$ at time t, which includes the sensor security and energy states $[s_{(n)}(t), e_{(n)}(t)]$. Each state represents the security condition and the residual battery energy level of sensor n at time t. For example, security state space I can include two security

levels: $\{safe, compromised\}$. The residual battery energy of each sensor can be divided into h discrete levels. Therefore, the residual energy state space E includes energy $\{e_1, \ldots, e_h\}$.

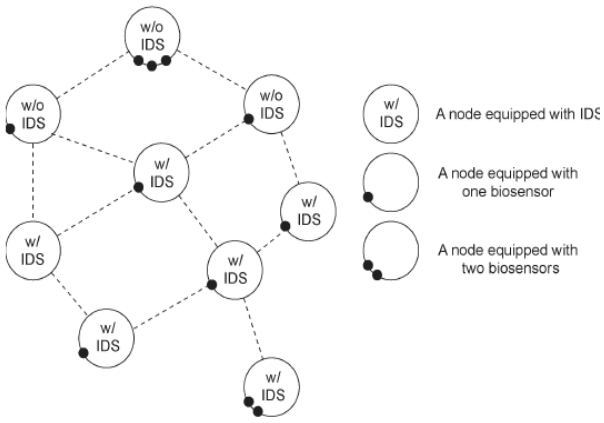

Fig 1. An example framework for the MANET with biosensors and IDSs

III. SYSTEM MODEL

Assume that a MANET has a continuous biometric-based authentication system with N −W biosensors and W IDSs, which have the ability to detect intrusions. The IDSs are also modeled as sensors, bringing the total number of sensors to N. Without loss of generality, we assume that some nodes have one or more biosensors, and some have no biosensor due to the heterogeneity of network nodes in the MANET. Similarly, some nodes are equipped with the IDS, and some are not equipped with the IDS. The total number of network nodes in the MANET is not directly related to the number of sensors. An example framework for the MANET with biosensors and IDSs is shown in Fig. 1.

The system can perform two kinds of operations:

1) intrusion detection
2) user authentication.

In the proposed scheme, since each sensor (biosensor or IDS) has measurement and estimation limitation, more than one biosensor and IDS (assume L devices) is chosen to detect the security states of the system. Each sensor monitors its local environment and not other sensors'. Then, their observations can be fused to increase observation accuracy using Dempster–Shafer theory[3]. The number of sensors chosen is determined by the required level of network performance. In the proposed scheme, a Markov model is used. Let the state of an arbitrary sensor n {1, 2, . .,N} be $x^{(n)}(t)$ at time t, which includes the sensor security and energy states $[s^{(n)}(t), e^{(n)}(t)]$. Each state represents the security condition and the residual battery energy level of sensor n at time t. For example, security state space can include two security levels: {safe, compromised}[11]. The residual battery energy of each sensor can be divided into discrete levels. Therefore, the residual energy state space E includes energy states {e1, . . . , eh} . Let $x_k^{(n)}$, $s_k^{(n)}$ and $e_k^{(n)}$ denote the state of sensor n, its security state, and its residual energy state, respectively, at discrete time k = 0, 1, ... States $s_k^{(n)}$ and $e_k^{(n)}$ evolve based on state and E-state Markov chains with transition probability matrices $U^{(n)}$ and $V^{(n)}$, respectively, if sensor n is used at time k, which are described as follows:

$$U^{(n)} = (\varphi^{(n)}_{ij})_{i,j} \in I \quad (1)$$

$$V^{(n)} = (\psi^{(n)}_{ij})_{i,j} \in \varepsilon \quad (2)$$

$\varphi^{(n)}_{ij} = P(s_{k+1}^{(n)} = j \mid s_k^{(n)} = i)$ (3)

$\psi^{(n)}_{ij} = P(e_{k+1}^{(n)} = j \mid e_k^{(n)} = i)$ (4)

Table I Main Notations

Symbols	Notations
$s_k^{(n)}$	The Security state of sensor N
$e_k^{(n)}$	The residual energy state of sensor n at time slot K
$U^{(n)}$	The State Transition probability matrix of the security state of the sensor n
$V^{(n)}$	The State Transition probability matrix of the residual state of the sensor n

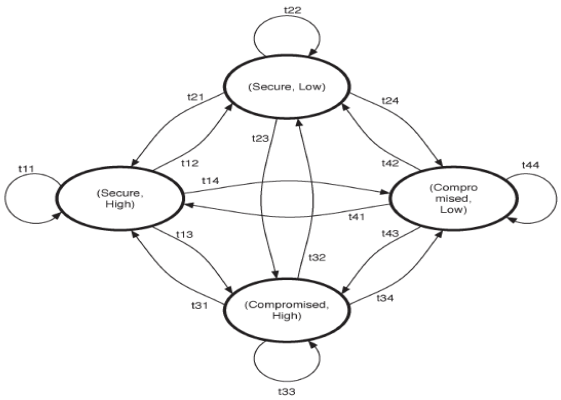

Fig 2 Example of Marcov chain's for a single node's state transition

The states of other idle sensors are unchanged, i.e.,

$s^{(n)}_{k+1} = s^{(n)}_k$ &

$e^{(n)}_{k+1} = e^{(n)}_k$, if sensor n is idle at time k. Hence, the state of sensor n transitions with probability matrix $T^{(n)}(n) = [U^{(n)} \otimes V^{(n)}]$, where $\otimes$ denotes the Kronecker product. For example, if there are two security states and two energy states, the state transition probability matrix of each sensor is a 4 * 4 matrix, whose Markov chain is shown in Fig. 2

IV. DEMPSTER SHAFER EVIDENCE THEORY

The Dempster–Shafer evidence theory[5] was originated by Dempster and later revised by Shafer. Its essential idea is that an observer can obtain degrees of belief about a proposition from a related proposition's subjective probabilities. The motivation for selecting Dempster–Shafer theory to solve the fusion problem in our proposed scheme is given as follows .

1) It has a relatively high degree of theoretical development for handling uncertainty or ignorance.
2) It provides a convenient numerical procedure for combining disparate data obtained from multiple sources.
3) It is widely used in various applications.

In a Dempster–Shafer reasoning system, a set of mutually exclusive and exhaustive possibilities is enumerated in the frame of discernment, which is denoted by Ω . In this section, two security states for each node, i.e., {secure, compromised}, are used to demonstrate how to use Dempster–Shafer theory in the fusion of biometric sensors and IDSs. In the proposed scheme, the frame of discernment consists of two possibilities concerning the security state of an arbitrary node a. That is, Ω = {secure, compromised}, which presents that node a has two security states:

1) secure state
2) compromised state.

Any hypothesis H refers to a subset of Ω for which the neighboring biometric sensors and IDSs can present evidence. The set of all possible subsets of Ω, including itself and the null set, is called a power set and is designated as 2Ω . For Ω in the proposed scheme, the power set has three focal elements:

1) hypothesis H = {secure};
2) hypothesis H^ = {compromised};
3) hypothesis U = Ω,

which means that the observed sensor a is either in the secure state or the compromised state. Each biometric sensor and IDS contributes its observation by assigning its beliefs over Ω

In this paper, if a sensor is trustworthy, then the sensor always provides accurate observation data. Any chosen node could be untrustworthy due to its current compromised state or inaccurate detection. The chosen node n is trustworthy for an arbitrary observed node a at time slot k + 1 when it is in the securestate and accurately detects[3]. The trustworthy probability $tp^{(n)}_{k+1}$ of node n at time k + 1 is equal to

$P(s^{(n)}_{k+1} = \text{secure}) \times P(y^{(n)}_{k+1} = s^{(a)}_{k+1})$ (5)

where $y^{(n)}_{k+1}$ is the observation of a's security state obtained from node n.

In this scheme,

$P(y^{(n)}_{k+1} = \text{secure} | s^{(a)}_{k+1} = \text{secure})$ (6)

$P(y^{(n)}_{k+1} = \text{compromised} | s^{(a)}_{k+1} = \text{compromised})$ (7)

are equal to 1 − FAR and 1 − FRR, respectively. FAR and FRR are the frequencies of FA errors and FR errors for node n, respectively. Otherwise, node n is not trustworthy with probability $1 - tp^{(n)}$ k+1. Suppose that node n states that node a is secure. If node n is trustworthy, then its claim is accurate. If n is not trustworthy, its claim is not necessarily inaccurate. Basic probability assignment reflects the evidence's strength of support . For example, for node n, the basic probability number $m_n(H)$ is defined as the portion of total belief assigned to hypothesis H. When n's observation data $y^{(n)}_{k+1}$ for the security state of node a at time k + 1 are equal to secure, its basic probability assignment[6] can be calculated

$m_n(H) = P(s^{(n)}_{k+1} \text{ secure}) \times P(y^{(n)}_{k+1} = \text{secure} | s^{(a)}_{k+1} = \text{secure})$ (8)

$m_n(H^\wedge) = P(s^{(n)}_{k+1} \text{ secure}) \times P(y^{(n)}_{k+1} = \text{secure} | s^{(a)}_{k+1} = \text{compromised})$ (9)

$m_n(U) = P(s^{(n)}_{k+1} = \text{compromised})$ (10)

If node n claims that node a is compromised, its basic probability assignment can be calculated as follows :

$m_n(H) = P(s^{(n)}_{k+1} \text{ secure}) \times P(y^{(n)}_{k+1} \text{ compromised} = | s^{(a)}_{k+1} = \text{secure})$ (11)

$m_n(H^{\wedge}) = P(s^{(n)}_{k+1}$ secure)× $P(y^{(n)}_{k+1}$ = compromised $|s^{(a)}_{k+1}$ = compromised) (12)

$m_n(U) = P(s^{(n)}_{k+1}$ = compromised) (13)

V. DEMPSTER SHAFER WEIGHTED EVIDENCE COMBINING RULE

Dempster-Shafer weighted evidence combining rule [11] is used in Dempster–Shafer evidence combination. Based on the historical performances of the sensors in similar situations, their corresponding correctness rates are used as the references to decide how much the sensors' current estimations should be trusted from their current observation. Let w_b and w_c be the corresponding estimation correctness rates in history for b and c respectively. Then, the combined belief of biometric sensors b and c can be calculated as follows

$m_b(H) \oplus m_c(H) = 1/K\ [w_b m_b(H) w_c m_c(H) + w_b m_b(H) w_c m_c(U) + w_b m_b(U) w_c m_c(H)]$ (14)

$m_b(H^{\wedge}) \oplus m_c(H^{\wedge}) = 1/K[w_b m_b(H^{\wedge}) w_c m_c(H^{\wedge}) + w_b m_b(H^{\wedge}) w_c m_c(U) + w_b m_b(U) w_c m_c(H^{\wedge})]$ (15)

$m_b(U) \oplus m_c(U) = 1/K[\ w_b m_b(U) w_c m_c(U)]$ (16)

where $K = 1 - w_a w_b m_a(H) m_b(H^{\wedge}) + m_a(H^{\wedge}) m_b(H)$

VI. DATA FUSION

L sensors are chosen for authentication and intrusion detection at each time slot to observe the security state of the network[9].To obtain the security state of the network, these observation values are combined, and a decision about the security state of the network is made. However, since there is some probability that a given sensor might either be in a compromised state or have made an inaccurate assessment, it is possible that this sensor has contributed an unreliable observation.

Type-I classifier[5] output single-class labels (SCLs). Majority voting and behavior-knowledge space are two most representative methods for fusing SCL classifiers. Majority voting can operate under the assumption that most of the observing nodes are trustworthy.

Type-II classifiers output class rankings. Two major fusion methods of type-II classifiers' outputs are based on either a class set reduction (CSR) or a class set reordering (CSRR). CSR methods try to find the minimal reduced class set, in which the true class is still represented. CSRR methods try to increase the true class ranking as high as possible.

Type-III classifiers produce so-called soft outputs, which are the real values in the range [0, 1]. Fusion methods for type-III classifiers try to reduce the uncertain level and maximize suitable measurements of evidence.

VII. GITTINS INDEX RULE

It means that the scheduling problem only needs to solve the individual POMDPs [8] for each sensor. Therefore, the computational complexity of the proposed scheme dramatically decreased For online real-time scheduling of different sensors, each sensor just looks up the prebuilt index table to find the index value corresponding to the current state. A lookup table can be designed with little computational complexity. In addition, several computationally efficient algorithms can be found in to further reduce the computational complexity of the proposed scheme.

VIII.. EXPERIMENTAL RESULT

The results show that the proposed scheme with data fusion and the proposed scheme without data fusion have lower cost and less information leakage than the existing scheme. Thus, through optimal node selection, the system can be more secure and energy efficient. From these figures, we can observe that data fusion can improve performance. The reason the fusion scheme has better performance is that data fusion using Dempster– Shafer theory increases the observation accuracy by combining the observations from multiple sensor.

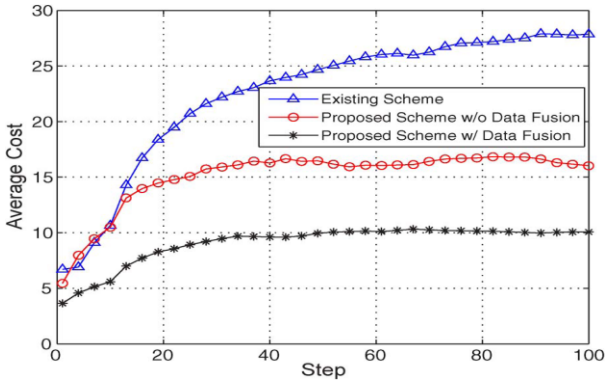

Fig 4.Information Leakage comparision among the three schemes

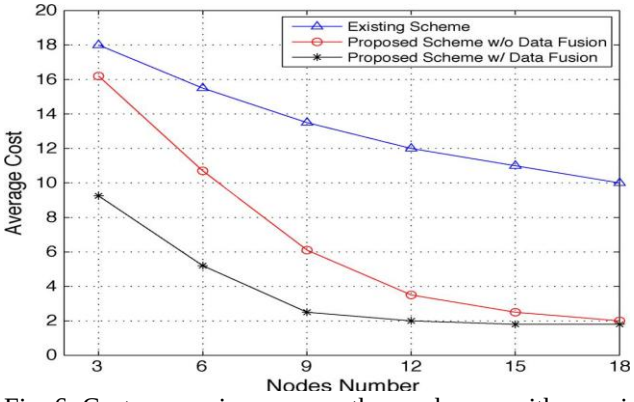

Fig. 6. Cost comparison among three schemes with varying nodes in the network.

IX. FUTURE WORK

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.

X. CONCLUSION

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 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. The problem has been formulated as a POMDP multiarmed bandit problem, and its optimal policy can be chosen using Gittins indices. 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] Y. Zhao, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," IEEE Trans. Dependable Secure Comput., vol. 3, no. 4, pp. 386–399, Oct.–Dec. 2006.
[2] B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu, and S. Guizani, "A pyramidal security model for large-scale group-oriented computing in mobile ad hoc networks: The key management study," IEEE Trans,vol. 58, no. 1, pp. 398–408, Jan. 2009.
[3] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 687–700, Apr. 2007.
[4] Q. Xiao, "A biometric authentication approach for high security adhoc networks," in Proc. IEEE Inf. Assur. Workshop, West Point, NY, Jun. 2004, pp. 250–256.
[5] J. Koreman, A. C. Morris, D. Wu, and S. A. Jassim, "Multi-modal biometrics authentication on the secure phone PDA," in Proc. 2nd Workshop Multimodal User Authentication, Toulouse, France, May 2006.
[6] S. K. Das, A. Agah, and K. Basu, "Security in wireless mobile and sensor networks," in Wireless Communications Systems and Networks. New York: Plenum, Jan. 2004,
pp. 531–557.
[7] A. Altinok and M. Turk, "Temporal integration
for continuous multimodal biometrics," in Proc. Workshop Multimodal User Authentication Santa Barbara, CA, Dec. 2003.

[8] J. Muncaster and M. Turk, "Continuous multimodal authentication using dynamic Bayesian networks," in Proc. 2nd Workshop Multimodal User Authentication, Toulouse, France, May 2006.
[9] J. Liu, F. Yu, C. H. Lung, and H. Tang, "Optimal combined intrusion detection and biometric-basecontinuous authentication in high security mobile ad hoc networks," IEEE Trans. Wireless Commun., vol. 8, no. 2, pp. 806–815, Feb. 2009.
[10] V. Krishnamurthy and B. Wahlberg, "Partially observed Markov decision process multiarmed bandits—Structural results," Math. Oper. Res., vol. 34, no. 2, pp. 287–302, May 2009.
[11] H. Wu, "Sensor fusion for context-aware computing using Dempster-Shafer theory," Ph.D. dissertation, Carnegie Mellon Univ., Pittsburgh, PA, 2003.

S.Jeyashree received B.Tech degree from Anna University, Chennai, Tamilnadu, India in the year 2010 in the area of Information Technology. Doing M.E in the area of Computer Science and engineering under Anna University, Chennai, Tamilnadu, India. She is working as a lecturer in Sree Sowdambika College of Engineering (affiliated by Anna University, Chennai) Aruppukottai, Tamilnadu, India. She is a member of CSI chapter.