MHIDCA: Multi Level Hybrid Intrusion Detection and Continuous Authentication for MANET Security

Soheila Mirzagholi[a], Karim Faez[b*]

[a] *Faculty of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran*
[b] *Electrical Engineering Department, Amirkabir University of Technology, Tehran, Iran*

Received 10 September 2015; accepted 1 November 2015

Abstract

Mobile ad-hoc networks have attracted a great deal of attentions over the past few years. Considering their applications, the security issue has a great significance in them. Security scheme utilization that includes prevention and detection has the worth of consideration. In this paper, a method is presented that includes a multi-level security scheme to identify intrusion by sensors and authenticates using biosensors. Optimizing authentication and intrusion detection combination, we formulate the problem as a partially observable distributed stochastic system. In order to reduce the computation time, the parallel forward algorithm of Hidden Markov Model has been used. Due to the possibility of misdetection of the sensor and in order to increase the accuracy of observations, more than one sensor is selected in every step, the observations obtained from the sensors are combined for more accurate identification, and the system decides about the security status based on combined observations of the sensors. Bayesian theory has been used in sensors evidence fusion brought by increased accuracy and network security, which will be observed in the simulations. The use of this theory causes the increase of accuracy and security on networks.

Keywords: Security, Mobile ad-hoc Networks, Authentication, Intrusion Detection, Hidden Markov Model.

1. Introduction

Within the recent years, MANETs have attracted a great deal of attention to their features of self-configuration and self-organization. These networks are formed without any predetermined infrastructure, where the mobile devices in them are connected to each other by wireless connections [1]. Security has most importance in MANETs. Unlike wired networks that are intrinsically secure, MANETs are not secure enough due to lack of management and central control as well as shared wired media. In MANETs, a security scheme consists of prevention, detection, and reaction, where authentication is the most important component for maintaining the security of the network since it is the first step to access a system in the network [2]. Authentication is the process of confirming the identity of a user. In risky environments or anywhere that the cost of unauthorized access to a computer is important, confirmation of the account does not occur only in entrance to the system, but is carried out

* Corresponding author. Email: kfaez@aut.ac.ir

continuously. One of the effective approaches for continuous authentication is employing biometric-based security. Biometrics provides some solutions for continuous authentication such as fingerprint and iris detection should have been explained in introduction [3]. Since biometrics does not require transportation of a device for continuous authentication, they are favorable. However, they are not sufficient for maintaining the security of a system. For example, an invalid gesture results in failures in the face detection, for which multimodal biometrics have been proposed that develop the accuracy and reduce the vulnerability [4].

Nowadays, Intrusion Detection Systems (IDSs) are known as an important and available technology in the security of mobile ad hoc networks, as the intrusion prevention techniques cannot maintain the system security on their own. In every security scheme, intruder locating provides the system with the time, type, and action of the intrusion as well as the layer in which intrusion has happened. There are three detection systems: network-based IDSs, host-based intrusion detection systems, and router-based IDSs. In MANETs, the host-based detection systems are used, because in these networks no entry or centralized router might be present [5]. A method for detecting and locating spoofing attacks in the mobile wireless environment and also to develop a Distance based Attack Localization and Detection (DALD) system, which is based on the distance of each packet while travelling from source to destination and where every node alert its neighbors[6].

In study carried out in [7], the main focus has been on authentication and intrusion detection by fusion the observation on MANETs. To overcome unimodal systems, multimodal biometrics have been used where Dempster-Shafer theory has been employed for fusion of observations. Research conducted in [8] has dealt with an advanced authentication technology based on biometric techniques and the cross-sectional behavior of users. In this scheme, intrusion detection and authentication approaches have been considered in both traditional and third-generation mobile networks. Research in [9] has been devoted to propose a novel security structure to protect information in MANETs by several security behaviors together with low computational complexity. The majority of attempts in the problem of combining intrusion detection and authentication are related to lowering the computational time of the relevant algorithm and increasing the system accuracy. In [10], some researches have been carried out regarding biometric-based continuous authentication benefiting from Bayesian networks for authentication. In [11], an architecture and implementation have been presented for multimodal biometric authentication systems together with new criteria for testing this system. In [12], using fuzzy controllers, a user continuous authentication method by aggregating temporal and spatial information has been proposed. In [13] a pre-processing method has been presented to improve Hidden Markov Model (HMM) for detection of host-based anomalies. In [14], continuous authentication and intrusion detection have been considered conjunctively to improve the security of MANETs. The authors in this study have utilized multimodal biometrics for continuous authentication and used IDS for detection of the system security status. Reducing computational time has also been addressed in this research.

In order to combine authentication and intrusion detection, in [9] the entire network has been formulated as a partially observable Markov decision process (POMDP) [15]. This scheme has been solved in a centralized way. However, in the method available in this study, in order to obtain the optimal combination scheme of intrusion detection and authentication, the problem has been dealt with in a distributed way and formulated as a partially-observed distributed statistical system [16]. Moreover, multi modal biometrics has been used instead of one-dimensional biometrics in order to mitigate the weakness of the system. In the present research, since every sensor has a limited estimation and measurement range, more than one sensor is chosen for detection of the system security status. The nodes sense the changes in the region cooperatively, which when combined, can give a more accurate view in comparison with MANET, preventing from vulnerability of the network to failure of one node. The observations obtained from the sensors are combined with Bayesian data fusion theory to improve the accuracy of the system. The numbers of selected sensors were combined to contingent upon the performance level of the network. As every sensor has a limited energy due to energy constraints of the sensors, to reduce the computational time of combining intrusion detection and authentication, the parallel algorithm of Hidden Markov Model is used. The rest of the paper organized as follows. Section 2 deals with description of the basic concepts of the problem. Then, in Section 3, the proposed method is explained, in which Bayesian theory and the Hidden Markov parallel forward algorithm is outlined. Section 4 presents the results of the experiments to determine efficiency of the proposed method.

2. Basic Concepts

In this paper, Assume that a MANET has a biometric-based continuous authentication system with N − W biosensors and W IDSs. The IDSs are modelled as sensors bringing the total number of sensors to N. The sensors are used as systems for intrusion detection and authentication [15]. The total number of sensors is N. Without loss of generality, we assume that some nodes have one or more biosensors, while some of them have no biosensors. Some nodes are equipped with both fingerprint and iris sensors resulting the heterogeneity in the network nodes in MANET. Similarly, some nodes are equipped with IDS, while others are not. The total number of network nodes in MANET is not directly related to the number of sensors. Figure 1 represents a framework of MANET with the sensors. The time has been divided into equal sections in the system. In the proposed system, authentication and intrusion detection processes are carried out. Authentication is done in every time section, where the intrusion detection system supervises the system throughout all time sections. In the proposed scheme, HMM is used for the decision-making process. We formulate the scheduling problem as a stochastic partially observed Markov decision process (POMDP) multi-armed bandit system, which is a powerful framework to solve the distributed optimization problem. Let the state of a sensor n, n ∈ {1, 2. . . N}, are at the time of containing Sensor security and energy states of. The security state of every sensor is divided into two states of {secure and compromise}. Likewise, the energy state of every sensor is categorized into two states of {high and low energy}. In response to the transfer probability matrix of every sensor, a 4*4 matrix whose Markov chain is shown in Fig. 2, the energy state space and security state space are defined. The time axis is also divided into equal sections including the time interval between two continuous authentications of the user [10]. Represents the sensor energy state at the discrete time of k {k=0, 1, 2,} and denotes the security state of sensor n at the time of k. Are states with transfer probability matrix of V^n and U^n, according to Markov chain of ε and I?

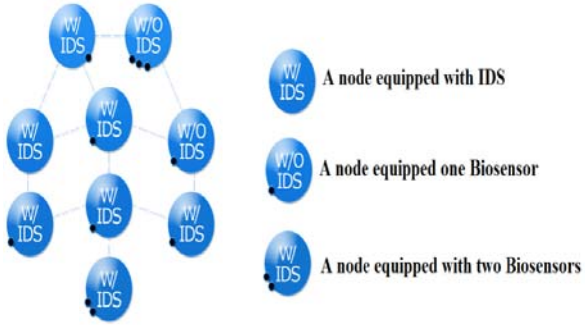

Fig. 1.An example of MANET framework with sensors [17]

$$\varphi_{ij}^{n} = p(s_{k+1}^{n} = j \mid s_{k}^{n} = i) \qquad U^{n} = (\varphi_{ij}^{n})_{i,j\in I} \tag{1}$$

$$\phi_{ij}^{n} = p(e_{k+1}^{n} = j \mid e_{k}^{n} = i) \qquad V^{n} = (\phi_{ij}^{n}) i, j \in \varepsilon \tag{2}$$

The transfer probability matrix of T^n is calculated based on V^n and U^n. ϕ_{ij}^{n} Denotes the probability of transfer of sensor n from the security state of i to security state of j. U^n indicates the matrix of all of the transfer probabilities between states. φ_{ij}^{n} Denotes the probability of transfer of sensor n from the energy state of i to energy state j. V^{n} is representative of the matrix of all of the transfer probabilities between the states. In effect, the state of selected sensor n in MANETs are not directly observable. The energy and security states are specified by $y_{s,k+1}^{n}, y_{e,k+1}^{n}$, where they are indicative of the energy state observation of sensor n at the time of k+1 and the security state observation of sensor n at the time of k+1.The transfer probability matrix of the state of sensor n is specified by $T^{n} = U^{n} \otimes V^{n}$. $a_k = \{1,.....,N\}$ denotes the sensor selected at the time of k. the cost of information leakage is determined by $c_s(s_k^{a_k}, a_k)$ which is a representative of function of the security state of the sensor selected at the time of k, i.e. the information leakage cost of security state of sensor a_k at the time of k. It indicates that wrong authentication/intrusion detection has been shown totally correct and $c_e(e_k^{a_k}, a_k)$ which is a function of the energy state of the sensor selected at the time of k, i.e. the energy cost of sensor a_k at the time of k representing the energy cost expended for computation. If the sensor n is selected at the time of k, the total immediate cost will be equal to:

$$C(x_k^{n}, n) = (1-\lambda)c_s(s_k^{a_k}, a_k) + \lambda c_e(e_k^{a_k}, a_k) \qquad (3)$$

Which is equal to the sum of the cost of a_k security state at the time of k and energy state cost of this sensor at k. $\lambda \in (0,1)$ is weight function. For example, in a military MANET network, the weight factor is considered to be near zero, because information leakage is more important than energy shortage. In the proposed scheme, the total immediate cost of C_k at the time of k is defined as $C_k = \beta^{k} * C\left(x_k^{n}, n\right), n_{\neq} \{1,....,N\}$ and thus the total cost expected on a finite set is specified by (4) [13, 18].

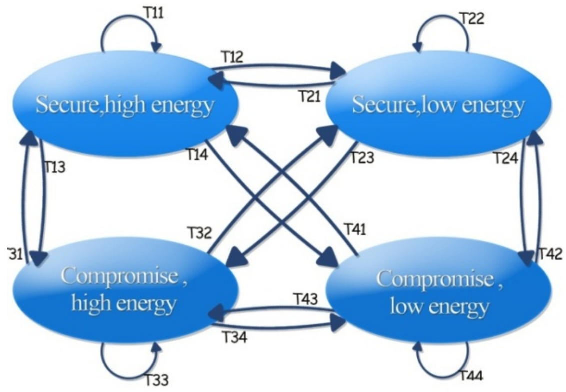

Fig. 2. A sample of Markov chain for transfer of a sensor state

$$J_{\mu} = E[\sum_{k=0}^{\infty} \beta^{k} (c(x_k^{(a_k)}, a_k))] \qquad (4)$$

β(0≤β<1) indicates the discount factor. This factor in turn reveals the fact that the future cost is less than the immediate cost, because confidence about the future is less. Now, in this system, reduced information leakage together with increased security levels is of importance. The observations obtained from these sensors are combined by Bayesian theory leading to increased accuracy of observation and security.

2.1. Formulation of the Information State

Since the state of a sensor is partially observable, selection of a sensor is not fully dependent on the current amount of observations and thus can be stated as a POMDP problem in the information state [17]. The information state of a sensor is related to probability distribution on the sensor states, where the total probability space to information space of is considered as the information state of sensor n at the time of k indicating that what the probability of sensor n at k would be at every state.

$$\pi_k^{n}(i), i = 1,....,\delta_n$$
$$\pi_k^{n}(i) = p(x_k^{n} = i \mid Y_k, A_{k-1}) \qquad (5)$$

Where, $\pi_k^{n}(i)$ represents the probability that the sensor n at k is in the state of i and shows the optimal action (intrusion detection/authentication) carried out at the time of K-1. x_k^{n} is the current state of the n$_{\text{th}}$ sensor, Y_k reveals the observations of the n$_{\text{th}}$ sensor at the time of k and A$_{k-1}$ indicates the action done at the time of K-1. If the sensor is chosen at k, the new observation of y_{k+1}^n will be obtained at the time of K+1. The information state of π_{k+1}^nknown reversibly by the forward algorithm of HMM, is then obtained, where the information state of other n-1 sensors not selected at the time of K+1, does not alter. The sensor selection algorithm in the next step is realized by the Gittins index (GI) which is an index-based optimal policy obtained from the following relation[18]:

$$\pi_k^n \gamma^n \{n = 1,\ldots,N\} \tag{6}$$

γ^n Denotes the cost vector of the n-th sensor. The optimal policy is to select sensors with the lowest GI at every step [14, 19]. If the number of sensors is large, the consumed energy and complexity of computation increased. In this paper, more than one sensor is chosen at every step, where the observations of sensors are combined with Bayesian theory.

3. The Proposed Method

In this paper, a multi-level structure has been proposed for combining intrusion detection and authentication. Re-authentication depends on the decision developed about the security state and the results of the intrusion detection of sensors. In Figure 3, after initial authentication for entrance to the system, L numbers of sensors are chosen randomly from the network by which intrusion detection is carried out. The observations obtained from these sensors are combined by Bayesian theory followed by decision-making about the security state. If it detects the combination results of the network as secure, then authentication with multimodal biometrics is no longer required (note that all nodes are authenticated in the initial entrance to the network with a hidden key), but when the network is not regarded as secure, authentication should be done.

Each sensor on its own has limited measurement and estimation capacity and monitors the local environment of itself rather than the environment of other sensors. In this regard, in order to obtain the network security state, more than one sensor is selected at every step for observation of the system security state in the proposed method. To achieve this, the values of the observations are combined by Bayesian theory developing a decision about the security state of the network. The number of sensors selected for combination should not be large due to computational consumed energy and complexity in combination of information, where authentication is dependent on the decision made about the security state.

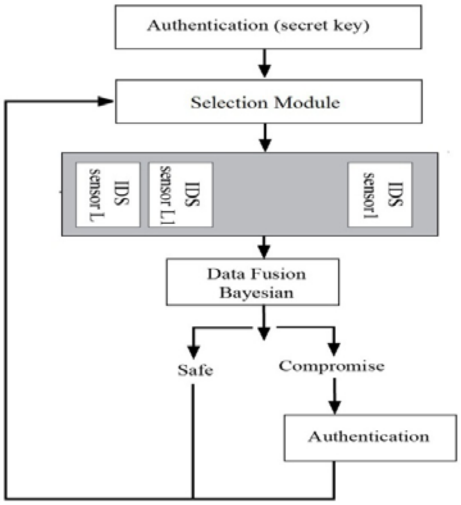

Fig. 3. The multi-level scheme of MHIDCA

In this paper, for the decision-making process, HMM has been employed. In the proposed scheme, since every sensor has limited consumed energy due to the energy limitation of sensors [19], to reduce the computational time of combining intrusion detection and authentication, we use parallel forward algorithm of HMM to achieve the system security state. The sequence of observations is distributed among the processors followed by aggregation of the results obtained from these processors. Moreover, by combination of the observations, the execution time does not increase, because the parallel forward algorithm of HMM has been utilized.

The security observations obtained from these sensors are then combined by Bayesian data fusion theory. Through combination of the observations of sensors, more accurate information can be obtained about the network, where we can achieve the network security state by taking the combined observations into account. Now, in the decision-making process, the obtained combined observations are considered as the inputs of parallel forward algorithm of HMM. Using this algorithm, the new information state is obtained followed by detection of the system security state.

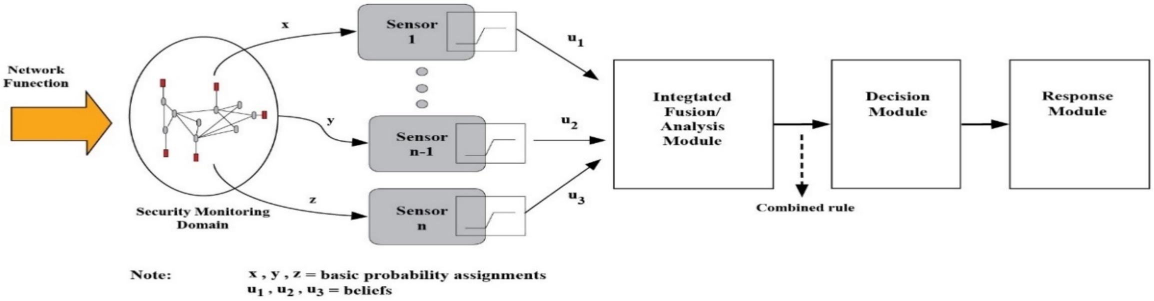

Fig. 4. Diagram of MHIDCA

Finally, the cost is calculated in the first step which is the amount of incorrect intrusion detection or authentication. The Gittins index of the selected sensors is calculated by Formula 6 and embedded into the GI vector. Next, L numbers of sensors with the lowest GI value are chosen, the observations of the L sensors are combined, and eventually the state of new information is obtained by these observations.

In this paper, two biosensors of fingerprint and iris have been considered for continuous authentication and IDS for intrusion detection in the network. Every sensor includes two energy states {high and low energy} and two security states {secure and insecure}. Overall, there are four states for each sensor according to Figure 2, where the intrusion detection sensor is considered as a sensor with low energy levels and minimum accuracy in detection of the security state, while iris sensor is regarded as a sensor with maximum consumed energy and the maximum accuracy in authentication.

3.1. Bayesian Data Fusion

To obtain the network security state, the observations are combined, followed by development of a decision about the network security state. If the selected sensor is in an insecure state and no accurate detection is made, the sensor might not have a reliable observation. Because the sensor might be out of operation or not have a correct measurement estimation. For example, consider the case where the state of the system is insecure, but the sensor detects the system as secure. Therefore selection of a proper data fusion method is of great importance. The probabilistic fusion method based on Bayesian rule is combined observation information. The Bayesian rule provides a concept for deductions regarding an object or environment with the data of x and z. It carries out a shared probability p (x, z) for separate or successive variables, where combination of n rules of conditional probabilities chain can be employed for development of shared probabilities. $p(x,z) = \mathrm{p(z \mid x)\,p(x)}$, for every x, the probability of realization of observing z is specified by $p(x \mid z)$ and for every fixed x, the probability of observing z. the new probabilities related to x are calculated and is obtained from the previous information and those gained through observations [20]. The conditional probability of $p(x \mid z)$ is used for a sensor and investigates the observations of a sensor. For cases when we employ several sensors and for combination of the observation of sensors in state x, we used

$$P(z_1,....,z_n \mid x) = p(z_1 \mid x)....p(z_n \mid x) = cp(x)\prod_{i=1}^{n} p(z_i \mid x) \qquad (7)$$

Where, c is a constant and the value of z_i is the observation of the i-th sensor with x indicating the state [21]. Figure 5 represents the stages of combination of sensors observation where first the observations of two sensors are combined which is in turn integrated with the observations of the third sensor.

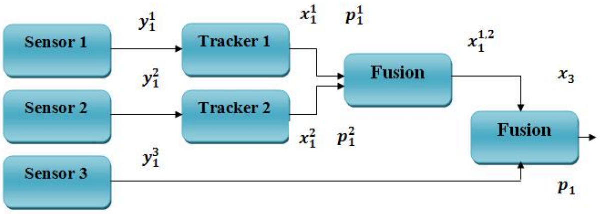

Fig. 5. Combined the observation of three sensors with Bayesian theory [10]

3.2. The Parallel Forward Algorithm of HMM

In this section, an improved forward algorithm is proposed with the aim of reducing computational complexity of the proposed scheme. A forward algorithm distributes observations among computational nodes independent of the data sequence length (observations). At the first level of the parallel approach, the observations are distributed among Power Processing Elements (PPE) by Message Passing Interface (MPI). The second level of paralleling is realized on Synergistic Processing Elements (SPEs) at which the forward probability of Hidden Markov Model is calculated. At every step of the parallel forward algorithm of HMM, the list of observations obtained from sensors are divided into some sections, each of which is further allocated to a processor. In every processor, the forward algorithm is run followed by aggregation of the results obtained from the processors. Figure7 demonstrates the sequential algorithm of HMM. In parallel implementation of the forward algorithm, as provided in Figure 6, the probability of the data distributed for PPE processors are calculated. Given the length of the sequence of information observation, every processor can run the forward algorithm simultaneously for sub-sequences, of which we have two in the present method. At this level where the sequence of observations has an equal distribution with the number of applied processors, MPI is used for parallel running of the algorithm.

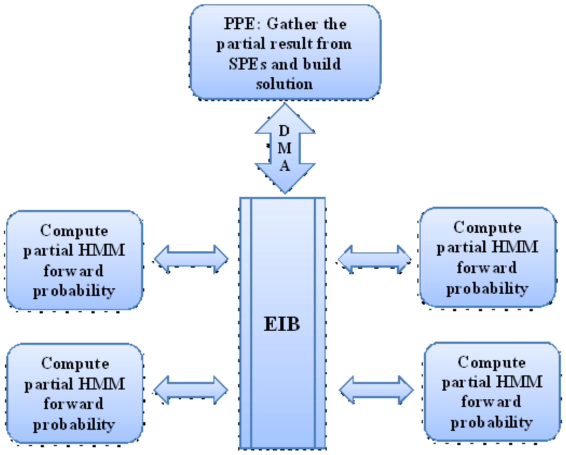
PPE: Gather the partial result from SPEs and build solution
D
M
A
EIB
Compute partial HMM forward probability
Compute partial HMM forward probability
Compute partial HMM forward probability
Compute partial HMM forward probability

Fig.6. The parallel approach of forward algorithm using MPI [19]

```
start
*)Read the HMM parameters $\lambda$ and observation sequences from file
*)Initialize  the probability $\alpha_1$
for  t=$o_2$,$o_T$ do
for i=1, N do
  for j=1, N do
   *)compute all probabilities $\alpha_T(j)$
      End for i
```

Fig. 7. The parallel forward algorithm of HMM [19]

Every processor of PPE has a number of sequences and calculates the forward probability of P data for a block of a sequence of the distributed observations. After calculation on every PPE processor, the MPI-send and MPI-receive functions are used for distribution/receiving the probability calculated on every processor. Eventually, the forward probability of the HMM model is obtained by aggregation of all of the cumulative probabilities from the processors [22].

4. Results and Discussion

In this section, MATLAB computer simulator has been used for evaluation of the performance of the proposed method. The transfer probability state matrix of the iris and fingerprint sensors and IDS are further provided. The matrix of observation probability of every sensor is equal to the transfer probability matrix of that considered sensor.

$$T_1 = \begin{bmatrix} 0.912 & 0.088 & 0.0 & 0.0 \\ 0.025 & 0.950 & 0.025 & 0.0 \\ 0.0 & 0.044 & 0.912 & 0.044 \\ 0.0 & 0.0 & 0.05 & 0.95 \end{bmatrix}$$

$$T_2 = \begin{bmatrix} 0.784 & 0.216 & 0.0 & 0.0 \\ 0.1 & 0.8 & 0.1 & 0.0 \\ 0.0 & 0.059 & 0.882 & 0.059 \\ 0.0 & 0.0 & 0.1 & 0.9 \end{bmatrix}$$

$$T_3 = \begin{bmatrix} 0.9702 & 0.0298 & 0.0 & 0.0 \\ 0.01 & 0.98 & 0.01 & 0.0 \\ 0.0 & 0.014 & 0.970 & 0.014 \\ 0.0 & 0.0 & 0.02 & 0.98 \end{bmatrix}$$

The primary state of every sensor has been considered $\pi = (1,0,0,0)$ signifying that every sensor lies in the state of {high energy and security} with the probability of 1, while the GI is regarded as a vector with zero elements. The cost vector of the iris and fingerprint sensors as well as IDS have been specified with C(1)=(3,8,20,40), C(2)=(2,7,22,45), and C(3)=(1,4,25,50), respectively, which have been applied in the simulations. The simulations are based on the comparison of the cost of the proposed method without and with combined observation. In this study, two sensors are chosen at every step whose observations are combined. The reason behind application of combined observation of two sensors has been the fact that by selecting more than two sensors at every step, the computational cost incurred by combined observations increases, so does the execution time of combination. In the preliminary stage, two sensors are chosen randomly, but in the next steps, the sensors with the lowest GI value are chosen. Then, the evidence obtained from these two sensors is combined by Bayesian theory. The reason of reduced cost in the proposed method in comparison with the method without combined observation is that in the proposed method, the observations probability obtained by the Hidden Markov Model is combined with the Bayesian theory, the transfer probability of sensors diminishes and thus the cost of information leakage drops as well. In addition, using the Bayesian theory, the accuracy of the observations grows by combining the observations from several sensors, because inaccurate detection by one sensor is highly probable and accordingly combined observation obtained from several sensors, more accurate data has been achieved.

In this paper, in order to reduce the execution time, the parallel forward algorithm of HMM [8] has been employed. At every step, this algorithm divides the list of observations obtained from the sensors into two sections allocating every section to one processor. In every processor, the forward algorithm is run followed aggregation of the results obtained from the processors at the end.

Table1.denotes consumed execution time by proposed method at 100 step for various number of sensors at MANET. As shown, this method reduces the execution time of continuous authentication and intrusion detection combination method. The results denote that proposed method is more effective and it reduces time of system.

Table 1

Result of MHIDCA with use of parallel forward algorithm HMM

	2 sensor	**4 sensor**	**20 sensor**	**50 sensor**
Result of [18]	*0.0427s*	*0.0576s*	*0.2337s*	***0.5960s***
Result of proposed scheme	*0.0195s*	*0.0349s*	*0.1397s*	***0.3575s***

Figure 8 illustrates the average cost for 100 steps by 40 sensors. As can be seen in the figure, in the proposed method, the average cost has declined over 100 steps. This is also caused by combination of evidence with the Bayesian theory that has brought about reduced cost as well as increased accuracy. This is in turn due to the fact that when a system becomes more secure, the cost decreases, since the proposed method prevents from selection of insecure nodes and in turn reduces the information leakage.

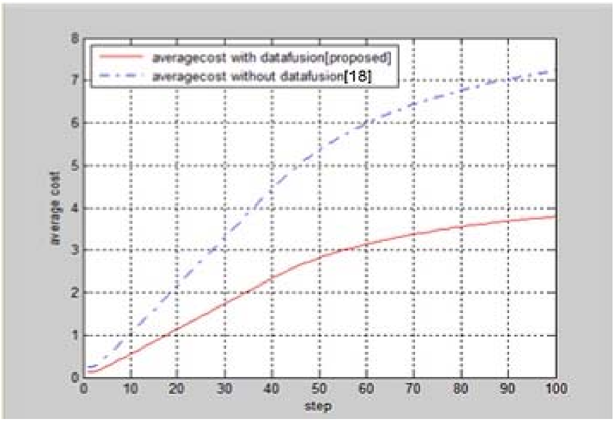

Fig. 8. The comparison between the average cost with and without combining the evidence.

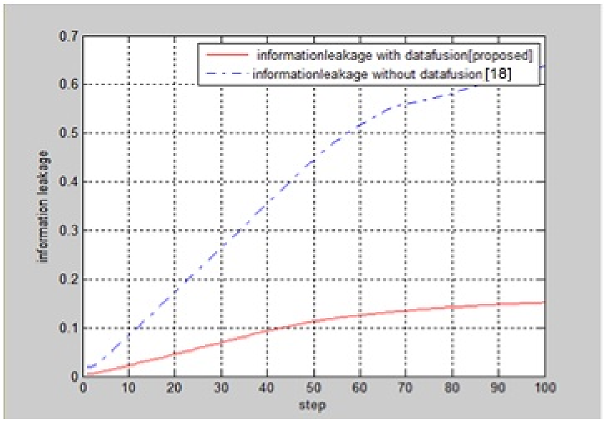

Fig. 9. The comparison between the information leakage with and without combining the evidence.

Figure 9 represents the information leakage for 100 steps, where information leakage is equal to the information leakage of the selected nodes divided by the leakage when nodes are in the worst state. This means that the average information leakage is obtained through sum of the cost of sensors divided by sum of the cost of sensors in the state of {low energy, low security}. As it can be observed in Figure 9, the proposed method has less information leakage suggesting that combination of data can improve the performance of the system. Our system becomes more secure and optimal in terms of energy consumption with another advantage being no prolongation of the execution time thanks to application of the parallel forward algorithm of HMM.

Figure 10 represent proposed method has lower cost than the Dempster-shafer data fusion [23] At the first steps, this discrepancy is more obvious but gradually the results to be together. it is concluded that, this method has higher accuracy rather than Dempster-shafer mean while at Bayesian data fusion method, we don't have unknown state and the states are completely clear, however with use of observation and event is choose again Dempster-shafer that may not give us clear result. Meanwhile Bayesian data fusion method is more understandable and simple than Dempster-shafer because it has less calculations at Bayesian data fusion method, we need primary information to start the work but as Dempster-shafer. This primary information is made. So we need to primary information such as we can use Bayesian data fusion.

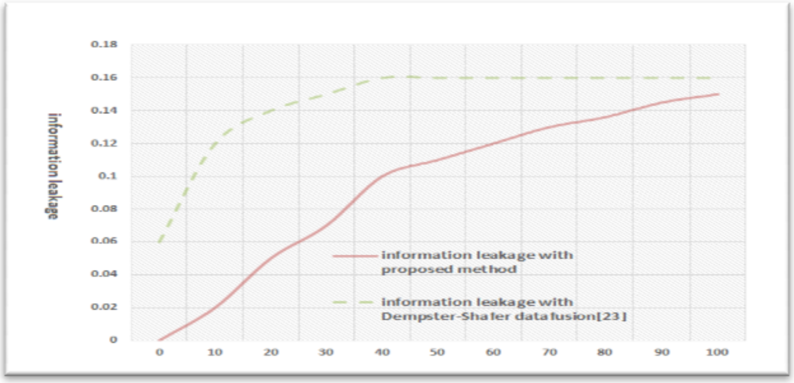

Fig. 10. The comparison between the information leakage with Dempster-shafer data fusion and Bayesian data fusion.

5. Conclusion

To improve the security in MANETs, combination of authentication and intrusion detection can be a suitable approach. Due to limitation of estimation and measurement of sensors, at every time section we have used the observations of several sensors to enhance the system accuracy. In this paper, we have used Bayesian theory for combined observations of sensors to promote the system accuracy. So as to reduce the system time, the parallel forward algorithm of HMM has been employed, bearing in mind that the system time does not increase by considering combined observations. The simulation results indicate that the proposed method can decrease the cost of information leakage in comparison with combination of authentication and intrusion detection without combined observations. In this paper, computational complexity increase with data fusion and it also reduces the system computational time by considering the parallel forward algorithm of HMM.

References

[1] P. A. P. v. Rajkumar P, Security Attacks and Detection Schemes in MANET, IEEE ICECS, Coimbatore. pp.1-6, (Feb 2014).

[2] S. D. M. I. Butun, "A Survey of Intrusion Detection Systems in wireless Sensor Networks" IEEE Communications Survay & Tutoria, 16(FIRST QUARTER 2014)1: 266-282.

[3] Q. Xiao, "A Biometric Authentication Approach For High Security Ad-Hoc Networks," Proc. IEEE Info. Assurance Workshop, West Point, NY, (Jun. 2004); 250-256.

[4] A. Rose, A. K. Jain, "Information Fusion in Biometrics," Pattern Recognition Letters, 24(2003):2115-2125.

[5] A. Mishra, K. Nadkarni, and V. T. A. Patcha, "Intrusion detection in wireless ad-hoc networks," IEEE Wireless Communications, (Feb. 2004):48–60.

[6] D. Sivakumar, B. Sivakumar. "Detection and Localization of Attackers in Wireless Networks."International Review on Computers and Software (IRECOS). (2014), 854-864.

[7] P. Dowland, S. Furnell, G. Magklaras, M. Papadaki, P. Reynolds, P. Rodwell, H. Singh," Advanced Authentication and Intrusion Detection Technologies", Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, UK.

[8] A. Tiwari," Intrusion detection & Prevention of Denial of Service Attacks in AODV Based MANET with Authentication Based Scheme", International Journal of Engineering Research &Technology,3 (April 2014)4.

[9] I. R. Stefania–IulianaSoiman, S.G. Pentiuc, "A parallel accelerated approach of HMM Forward Algorithm for IBM Roadrunner clusters," 12th International Conference on Development and Application Systems, Suceava, Romania, 2014.

[10] J. Muncaster, M. Turk, "Continuous MultiModal Authentication Using Dynamic Bayesian Networks," Second Workshop On Multimodal User Authentication, Toulouse, France, May 2006.

[11] T. Sim, S. Zhang, R. Janakiraman, S. Kumar, "Continue Verification Using Multi-Modal Biometrics," IEEE Trans. Pattern Analysis and Machin Intelligence, 29 (April 2007): 687-700.

[12] A. Azzini, S. Marrara, R. Sassi, F. Scotti, "A Fuzzy Approach to Multi-Modal Biometric Continuous Authentication," Fuzzy Optim Decis Making, 7(September 2008): 243-256.

[13] J. Hu, X. Yu, D. Qiu, "A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection," IEEE Network.23 (January 2009): 42-47.

[14] J. Gitten, "Multi-Armed bandit Allocation Indices," Whaley, (1989).

[15] V. K. a. B. Wahlberg, "Partially observed markov decision process multi armed bandits - structural result," math. of Oper. Res.34 (May 2009): 287-302.

[16] J. Liu, F. Yu, C. H. Lung, T. H, "Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication In High Security Mobile Ad-Hoc Networks," IEEE Trans. On Wireless Communications, 8(Feb.2009): 806-815.

[17] S. Jeyashree ,"Highly Secure Distributed Authentication and Intrusion Detection with Data Fusion in MANET" International Journal of Advanced Research in Computer Engineering & Technology, February 2013.

[18] R. Y. Shengrong Bu, Peter X.Liu, Helen Tang, "A Computationally Efficient Method for Joint Authentication and Intrusion Detection in Mobile Ad-Hoc Networks," Communications (ICC), Kyoto, jun.2011.

[19] H. Wu, "Sensor fusion for context-aware computing using Dempster Shafer theory," Carnegie Mellon Univ, 2003.

[20] V. K. a. R. J. Events, "Hidden Markov model multi armed bandits," IEEE Trans. Signal Process, 49(December 2001)12: 2893-2908,

[21] J.O. Berger: “Statistical Decision Theory and Bayesian Analysis “, Springer, Berlin, Heidelberg, 1985.

[22] K. K. Lakshmi Narayanan, A. Fidal Castro,” High Security for MANET Using Authentication and Intrusion Detection with Data Fusion” International Journal of Scientific & Engineering Research.3 (March 2012) 3.

[23] Bu. Shengrong, et al. "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks." Vehicular Technology, IEEE Transactions on.60 (2011)3: 1025-1036.