Distributed Combined Authentication and Intrusion Detection in High-Security Mobile Ad Hoc Networks to reduce the computation complexity

S.Parasakthi,
Assistant Professor,
Latha Mathavan Engineering College,
Madurai.

A.John Sanjeev Kumar,
Assistant Professor,
Thiagarajar College of Engineering,
Madurai.

ABSTRACT

Multimodal biometric technology provides potential solutions for continuous user-to-device authentication in high security mobile ad hoc networks (MANETs). This paper studies distributed combined authentication and intrusion detection with data fusion in such MANETs. Multimodal biometrics are deployed to work with Intrusion Detection Systems (IDS) to alleviate the shortcomings of unimodal biometric systems. Since each device in the network has 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 for data fusion. The system decides whether user authentication (or IDS input) 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. Simulation results are presented to show the effectiveness of the proposed scheme to reduce the Computation.

Index Terms

Authentication, biometrics, intrusion detection, mobile ad hoc networks (MANETs), security

1. INTRODUCTION

With recent advances in mobile computing and wireless communications, mobile ad hoc networks (MANETs) are becoming more attractive for use in military applications. Supporting security-sensitive applications in hostile environments has become an important research area for MANETs since MANETs introduce various security risks due to their open communication medium, node mobility, lack of centralized security services, and lack of prior security association. 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. The frequency depends on the situation severity and the resource constraints of the network. 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. Using this technology, individuals can be automatically and continuously identified or verified by their physiological or behavioral characteristics without user interruption.

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 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 (e.g., because of power control). Therefore, in the proposed scheme, energy consumption is also considered to improve the network lifetime.

2. LITERATURE SURVEY

2.1 Bo Rong, Hsiao-Hwa Chen, Yi Qian , Rose Qingyang Hu and Sghaier Guizani "A Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009 pp 398-408[21]

In mobile ad hoc networks (MANETs), many applications require group-oriented computing among a large number of nodes in an adversarial environment. To deploy these large scale cooperative applications, secure multicast service must be provided to efficiently and safely exchange data among nodes. The existing literature has extensively studied security protection for a single multicast group, in which all nodes are assumed to have the same security level. However, such an assumption may not be valid in practice because, for many applications, different users can play different roles and thus naturally be classified into multiple security levels. In this paper, we propose a pyramidal security model to safeguard the multisecurity-level information sharing in one cooperation domain. As a prominent feature, a pyramidal security model contains a set of hierarchical security groups and multicast groups. To find an efficient key management solution that covers all the involved multicast groups, the authors develop the following three schemes for the proposed security model:

1) separated star key graph; 2) separated tree key graph, and 3) integrated tree key graph. Performance comparison demonstrates that the scheme of integrated tree key graph has advantages over its counterparts.

2.2 Terence Sim, Member, Sheng Zhang, Rajkumar Janakiraman, and Sandeep Kumar "Continuous Verification Using Multimodal Biometrics" IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 29, NO. 4, APRIL 2007 pp 687-700 [22]

Conventional verification systems, such as those controlling access to a secure room, do not usually require the user to

reauthenticate himself for continued access to the protected resource. This may not be sufficient for high-security environments in which the protected resource needs to be continuously monitored for unauthorized use. In such cases, continuous verification is needed. In this paper, the authors present the theory, architecture, implementation, and performance of a multimodal biometrics verification system that continuously verifies the presence of a logged-in user. Two modalities are currently used—face and fingerprint—but their theory can be readily extended to include more modalities. We show that continuous verification imposes additional requirements on multimodal fusion when compared to conventional verification systems. We also argue that the usual performance metrics of false accept and false reject rates are insufficient yardsticks for continuous verification and propose new metrics against which we benchmark their system, continuously verifies the presence of a logged-in user. Two modalities are currently used—face and fingerprint—but their theory can be readily extended to include more modalities. We show that continuous verification imposes additional requirements on multimodal fusion when compared to conventional verification systems. We also argue that the usual performance metrics of false accept and false reject rates are insufficient yardsticks for continuous verification and propose new metrics against which we benchmark their system.

2.3 Jie Liu, F. Richard Yu, 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 pp 806-815 [23]

Two complementary classes of approaches exist to protect high security mobile ad hoc networks (MANETs), prevention-based approaches, such as authentication, and detection-based approaches, such as intrusion detection. Most previous work studies these two classes of issues separately. In this paper, the authors propose a framework of combining intrusion detection and continuous authentication in MANETs. In this framework, multimodal biometrics is used for continuous authentication, and intrusion detection is modeled as sensors to detect system security state. They formulate the whole system as a partially observed Markov decision process considering both system security requirements and resource constraints. They then use dynamic programming-based hidden Markov model scheduling algorithms to derive the optimal schemes for both intrusion detection and continuous authentication. Extensive simulations show the effectiveness of the proposed scheme.

In addition, further research is in progress to study the complexity of the combined system and to consider other responses initiated by an IDS in this framework

2.4 Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang "Securing Mobile Ad Hoc Networks with Certificateless Public Key"

IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 3, NO. 4, OCTOBER-DECEMBER 2006 pp 386-399 [24]

This paper studies key management, a fundamental problem in securing mobile ad hoc networks (MANETs). The authors present IKM, an ID-based key management scheme as a novel combination of ID-based and threshold cryptography. IKM is a certificateless solution in that public keys of mobile nodes are directly derivable from their known IDs plus some common information. It thus eliminates the need for certificate-based authenticated public-key distribution indispensable in conventional public-key management schemes. IKM features a novel construction method of ID-based public/private keys, which not only ensures high-level tolerance to node compromise, but also enables efficient network-wide key update via a single broadcast message. They also provide general guidelines about how to choose the secret-sharing parameters used with threshold cryptography to meet desirable levels of security and robustness. The advantages of IKM over conventional certificate-based solutions are justified through extensive simulations. Since most MANET security mechanisms thus far involve the heavy use of certificates, they believe that their findings open a new avenue towards more effective and efficient security design for MANETs.

3. MULTIMODEL BIOMETRIC-BASED USER AUTHENTICATION AND INTRUSION DETECTION

3.1 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 and
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) and
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 is 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.

3.2 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.

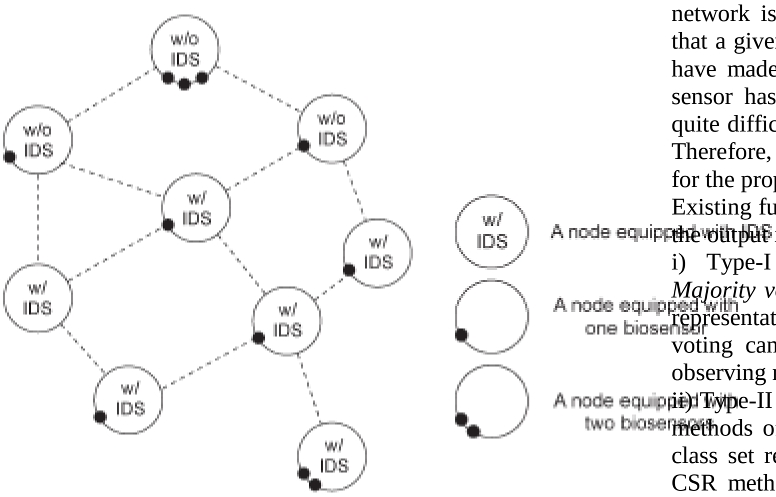

Figure 1. Example framework for a MANET with biosensors and IDSs.

3.3 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 theMANET is not directly related to the number of sensors. An example framework for the MANET with biosensors and IDSs is shown in Figure 1.

The system can perform two kinds of operations:

1) Intrusion detection and

2) user authentication.

The IDSs can operate at all time instants to monitor the system. Authentication may be executed at every time instant as well. However, intrusion detection and authentication may consume a large amount of energy, which is a concern for energy-constrained devices in MANETs.

4. DATA FUSION OF BIOMETRIC SENSORS AND INTRUSION DETECTION SYSTEMS

In the proposed scheme, L sensors are chosen for authentication 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 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. It can be quite difficult to ascertain which observers are compromised. Therefore, choosing an appropriate fusion method is critical for the proposed scheme.

In the proposed scheme, L sensors are chosen for authentication 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 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. It can be quite difficult to ascertain which observers are compromised. Therefore, choosing an appropriate fusion method is critical for the proposed scheme.

Existing fusion methods can be classified as follows based on the output information level of the base classifiers:

i) Type-I classifiers 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.

ii) 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.

Iii) 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. Fusion methods include Bayesian fusion methods, fuzzy integrals, Dempster–Shafer combination, fuzzy templates, product of experts, and ANNs.

5. FORMULATION OF THE DISTRIBUTED AUTHENTICATION AND INTRUSION DETECTION SCHEDULING PROBLEM

As we mentioned in the introduction, it is critical for the system to optimally schedule the intrusion detection and authentication activities for each time slot in a distributed manner, taking system security and energy into account. In this section, we formulate the distributed authentication and intrusion detection scheduling problem as a partially observable Markov decision process (POMDP) multiarmed bandit problem.

5.1 Information State Formulation

The decision about which sensors are chosen should not totally depend on the current observation values since the sensors' states are only partially observable. Therefore, all the actions and observations in the history should be counted as a basis for decision making under environmental uncertainties. To this end, information state is developed to derive sufficient statistical information for the past history, including all the actions and observations. The information state of a sensor refers to a probability distribution over the sensor's states. The entire probability space (the set of all possible probability distributions) is referred to as the information space.

5.2 Distributed Scheduling Process

To reduce the computational complexity of the proposed scheme, the distributed multimodal biometrics authentication and intrusion detection scheduling process can be divided into offline and online parts.

1) Offline computation of Gittins index. As with any dynamic programming formulation, the computation of the Gittins index for each sensor can be done offline For an arbitrary sensor n, a set of vectors Λ(n) k at each iteration k is computed in advance based on the following parameters: state transition probability matrix T(n), observation probability matrix B(n), reward vector R(n),
initial information state π(n) 0 , horizon length H, and discount factor β.

2) Real-time sensor selection over horizon H. At time k, each sensor stores the sensors' current Gittins indexes into an N-dimensional vector. The real-time sensor selection includes the following steps.

a) Select L sensors with the highest Gittins indexes at time k. For these L sensors, perform steps a to e.

b) Get new sensor observations $y_{k+1}^{(n)}$ at time k + 1.

c) Update the information states of the L chosen sensors using the corresponding HMM filters.

d) Compute the Gittins index $\gamma_H^{(n)}(\pi_{k+1}^{(n)})$ for each of these L sensors only.

e) Broadcast the new Gittins indexes to the other sensors.

f) On receiving the messages, all the sensors update their Gittins indexes. Go to step a.

5.3 Discussion of Computational Complexity andCommunication Overhead

In the proposed scheme, the optimal policy can be found by a Gittins index rule, which means that the scheduling problem only needs to solve the individual POMDPs for each sensor. Therefore, the computational complexity of the proposed scheme is 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. For example, based on Lovejoy's suboptimal algorithm, the value function can be upper and lower bounded, and efficient suboptimal
solutions can be developed. Finally, by imposing structural assumptions on the state transition probabilities, cost vectors, and observation probabilities, some structural policies (e.g., threshold policy) can be derived.

In the proposed scheme, communication overhead is mainly due to multicasting the following two types of messages in the real-time scheduling process:

1) INTIAL-SENSOR-INDICES (ISIND), 8 bytes, which is sent at the beginning of the authentication and intrusion detection process, so that each sensor knows the others' Gittins indexes;

2) SENSOR-INDICES (SIND), 8 bytes, which is sent at the beginning of each time slot by the *L* nodes active in the previous time slot.

6. SIMULATION RESULTS AND DISCUSSIONS

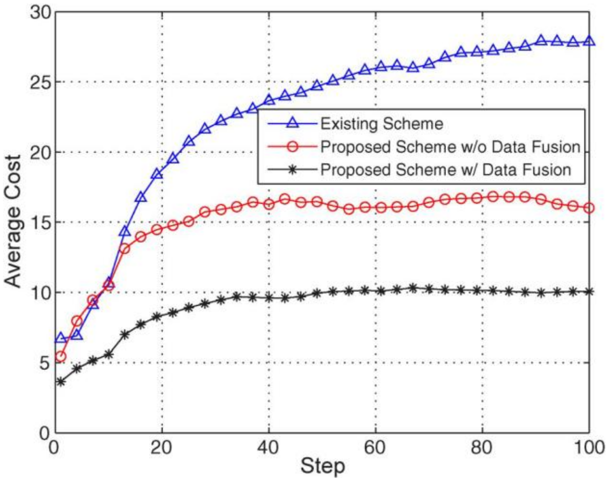

Figure 2. Cost comparison among the proposed scheme with data fusion, the proposed scheme without data fusion, and the existing scheme

We run simulations to compare the cost of three approaches: 1) the proposed scheme with data fusion; 2) the proposed scheme without data fusion; and 3) a scheme that does not consider optimal scheduling (that is, a scheme that randomly makes selections). Each cost value is the averaged result of 10 000 simulations. Figure 2 shows the average cost for the first 100 steps of the simulation.

7. CONCLUSION AND FUTURE WORK

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 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. Such methods of combining multiple sensor information in a distributed fashion lend themselves well to the concept of cross-layer security, which is a topic that is gaining interest in MANET security.

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.

8. 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. Veh. Technol., 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-based continuous 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.

[12] A. Papanikolaou, C. Ilioudis, C. Georgiadis, and E. Pimenidis, "The importance of biometric sensor continuous secure monitoring," in *Proc. 3rd Int. Conf. Digital Inf. Manage.*, London, U.K., Nov. 2008.

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

[14] C. Katar, "Combining multiple techniques for intrusion detection," *IJCSNS Int. J. Comput. Sci. Netw. Security*, vol. 6, no. 2B, pp. 208–218, Feb. 2006.

[15] P. Hu, Z. Zhou, Q. Liu, and F. Li, "The HMM-based modeling for the energy level prediction in wireless sensor networks," in *Proc. IEEE Conf. Ind. Electron. Appl.*, Harbin, China, May 2007, pp. 2253–2258.

[16] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.—Special Issue on Biometrics*, vol. 2008, no. 113, pp. 1–17, Jan. 2008.

[17] P. Whittle, "Multi-armed bandits and the Gittins index," *J. R. Stat. Soc. Ser. B*, vol. 42, no. 2, pp. 143–149, 1980.

[18] J. Gittins, *Multi-Armed Bandit Allocation Indices*. Hoboken, NJ: Wiley, 1989.

[19] D. Ruta and B. Gabrys, "An overview of classifier fusion methods," *Comput. Inf. Syst.*, vol. 7, pp. 1–10, 2000.

[20] T. M. Chen and V. Venkataramanan, "Dempster-Shafer theory for intrusion detection in ad hoc networks," *IEEE Internet Comput.*, vol. 9, no. 6, pp. 35–41, Nov. 2005.

[21] Bo Rong, Hsiao-Hwa Chen, Yi Qian , Rose Qingyang Hu and Sghaier Guizani "A Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009 pp 398-408.

[22] Terence Sim, Member, Sheng Zhang, Rajkumar Janakiraman, and Sandeep Kumar "Continuous Verification Using Multimodal Biometrics" IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 29, NO. 4, APRIL 2007 pp 687-700.

[23] Jie Liu, F. Richard Yu, 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 pp 806-815.

[24] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang "Securing Mobile Ad Hoc Networks with Certificateless Public Key"IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 3, NO. 4, OCTOBER-DECEMBER 2006 pp 386-399.