High Security for MANET using Intrusion Detection and Authentication with Data Fusion on Leaders

Fidalcastro. A
Research Scholar, Dept of CSE
Sathyabama University, India

Baburaj .E
Professor, Dept of CSE
Sun College of Engg &Tech, India

ABSTRACT
This paper proposes a novel architecture for security in Mobile Adhoc Networks using Intrusion Detection and Authentication with Data Fusion along with clustering technique and leader election model. Here clusters are formed through fixed width algorithm and it elects the leader node in each cluster with the help of neighbor ranking mechanism. Leader helps in finding out the intruder in the cluster and sends them out of the network by using Intrusion Detection System and Authentication device that are implemented only in leader node, so leader node is able to detect the intruder. To overcome the demerits in unimodal biometric system, Multimodal biometrics is set to work with IDS. Each and every device has dimensions and estimation limitations, many devices to be selected with the help of Dempster-Shafter theory for data fusion. Based on the security posture, system concludes which biosensor (IDS) to select and decide user need authentication (or IDS input) is essential. By every authentication device and Intrusion Detection System (IDS), the decisions are made in a fully distributed manner. Simulation results demonstrate that the novel architecture is efficient and accurate.

Keywords
MANET, Intrusion Detection System, Authentication, Leader election, Fixed width algorithm, Security

1. INTRODUCTION

Wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. Nodes within each other's radio range communicate directly via wireless links, while those that are out of range use other nodes as relays or routers. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band, and follow the same hopping sequence or spreading code.

Our proposed architecture using IDS and Authentication incorporates the security MANETs, users to 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.

Fixed width clustering algorithm [1] is implemented for anomaly detection engine for efficient detection of intrusion in the ad-hoc networks environment being captured is extremely high, authentication needs to be performed continuously and frequently.

Fixed width clustering algorithm [1] is implemented for anomaly detection engine for efficient detection of intrusion in the ad-hoc networks and also implemented leader election algorithm [3] in cluster group. The nodes in each cluster elect a leader node (cluster head) to serve as the IDS for the entire cluster. So IDS and Authentication device is implemented in leader node to detect the intruder.

The following scheme proposed in MANET with distributed nodes.

1) Clustering is formed through fixed with clustering algorithm
2) Leader selected through leader election algorithm.
3) IDS and Authentication is implemented in leader nodes. For authentication multimodal biometrics is deployed.
4) Leader nodes observations can be fused to increase observation accuracy. Dempster–Shafer theory [7] is used for data fusion.
5) The system decides [5] whether a user authentication (or IDS) is required and which biosensors should be chosen, depending on the security posture. The decisions are made in a fully distributed manner by each authentication device and IDS.
6) Since a biometric authentication process requires a large amount of computation, the energy consumption is significant. Due to the dynamic wireless channels in MANETs, the energy consumption for data transmissions is dynamically changing (e.g., because of power control).

2. RELATED WORK

Portnoy, L et.al [1], presented Fixed width clustering algorithm has shown to be highly effective for anomaly detection in network intrusion. Vasudevan, et.al [2] proposed leader election algorithm. Mohammed et.al [3] discussed to elect the leader in nodes of clusters. J.Liu, et.al [4], has discussed about IDS and Biometrics based authentication using a simple Hidden Markov Model. T.Sim et.al [5], has discussed about Continuous authentication for multimodel biometrics. Zhao.Y. et.al [6] has discussed about the certificate less keys (IKM) to secure the wireless network. T.M.Chen, et.al [7], has discussed about Dempster-Shafer theory for IDS. Mishra.A et.al [8], discussed the challenge for intrusion detection in ad-hoc network and purpose the use of anomaly detection. K.K. Lakshmi Narayanan and A. Fidal Castro, [9] discussed security on MANET using IDS and Authentication using data fusion. Rakesh Shrestha et.al [10] provides the clustering algorithm to form cluster within MANETS.

3. CLUSTER MECHANISM

Fixed-width clustering algorithm [1] is implemented for approach to anomaly detection. It calculates the number of points near each point in the feature space. In fixed width clustering technique, set of clusters are formed in which each cluster has fixed radius *w* also known as cluster width in the

feature space The cluster width *w* is chosen as the maximum threshold radius of a cluster.

3.1 Clustering Algorithm [1]

A set of network traffic sample ST (Samples Training) are obtained from the audit data for training purpose. Each sample si in the training set is represented by a *d*-dimensional vector of attributes. Si=<x1…….xd>. In the beginning, the set of clusters as well as the number of clusters are null. The number of clusters C:=0.Since, there is significant variation in each attribute. While calculating the distance between points, normalization ST is done before mapping into the feature space to ensure that all features have the same outcome. It is obtained by normalizing each continuous attribute in terms of the number of standard deviations from the mean. The first point of the data forms the centre of the new cluster. A new cluster 1 is formed having centroid 1 * from sample si. For every succeeding point, we measure the distance of each traffic sample si to the centroid of each cluster 1* that has been generated by the cluster set . If the distance to the nearest cluster n is within *w* of cluster center, then the point is assigned to the cluster, and the centroid of the closest cluster is updated. Else, the new point forms the centroid of a new cluster. Here We used fixed width clustering algorithm to form the clusters [1,10].

4. LEADER ELECTION ALGORITHM

Here used the Leader election algorithm [2,3] is to elect the most cost-efficient leaders with less performance overhead compared to the network flooding model. It devises all the needed messages to establish the election mechanism taking into consideration cheating and presence of malicious nodes and consider the addition and removal of nodes to/from the network due to mobility reasons. Finally, the performance overhead is considered during the design of the novel architecture where computation, communication, and storage overhead are derived.

4.1 Objectives and Assumptions

To design the leader election algorithm, the following are needed: 1) To protect all the nodes in a network, every node should be monitored by a leader 2)The overall cost of analysis for protecting the whole network is minimized. The Leader election model algorithm [3] is executed in each node, by consideration the following assumptions about the nodes and the network architecture:

- Each node knows its (2-hop) neighbors, which is reasonable, since nodes usually maintain a table about their neighbors for routing purposes.
- Loosely synchronized clocks are available between nodes.
- Each node is aware of the presence of a new node or Removal of a node.

4.2 Leader Election

To elect a new leader, the election algorithm [3] uses four types of messages. Hello, used by every node to initiate the election process; Begin-Election, used to announce the cost of a node; Vote, sent by every node to elect a leader; and Acknowledge, sent by the leader to broadcast its payment, and also as a confirmation of its leadership [3] .

Algorithm 1 (Executed by every node)[3]

On expiration of Timer T1, each node k checks whether it has received all the hash values from its neighbors. Nodes from whom the Hello messages have not received are excluded from the election. On receiving the Hello from all neighbors, each node sends Begin-Election, which contains the cost of analysis of the node, and then, starts timer T2. If node k is the only node in the network or it does not have any neighbors, then it launches its own IDS.

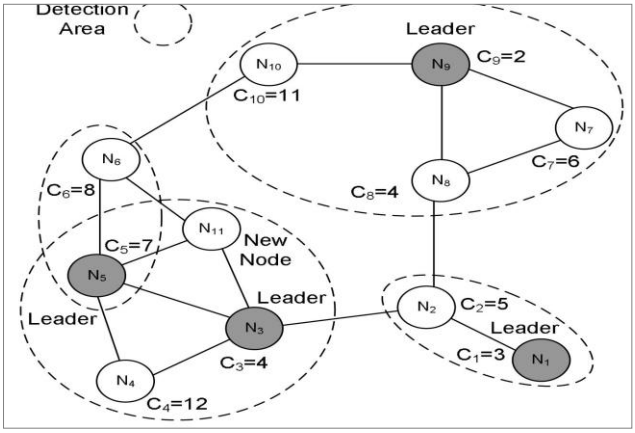

Fig.1: Leader Election

Algorithm 2 (Executed by every node) [3]

On expiration of T2, the node k compares the hash value of Hello to the value received by the Begin-Election to verify the cost of analysis for all the nodes. Then, node k calculates the least-cost value among its neighbors and sends Vote for node i. The Vote message contains the IDk of the source node, the IDi of the proposed leader, and second least cost among the neighbors of the source node cost j#i. Then, node k sets node i as its leader in order to update later on its reputation. Note that the second least cost of analysis is needed by the leader node to calculate the payment. If node k has the least cost among all its neighbors, then it votes for itself and starts timer T3.

Algorithm 3 (Executed by Elected leader node) [3]

Send Acknowledge message to the neighbor nodes.

Algorithm 4 (Executed by neighboring nodes) [3]

The neighboring nodes send 'Status' to new node.

Algorithm 5 (Executed by neighboring nodes) [3]

The neighboring nodes reconfigure the network and declare new election if necessary.

5. AUTHENTICATION AND INTRUSION DETECTION

In this section, biometric-based user authentication and IDSs are used in MANETs.

5.1 Authentication

Biometric technology [5] can be used to 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). In most real-world implementations of biometric systems [5], 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 proposed system to increase the effectiveness of user authentication

5.2. INTRUSION DETECTION SYSTEM

Intrusion detection is the most potential one because of its ability to detect new attacks. Many traditional intrusion detection [4] techniques are limited with collection of training data from real networks and manually labeled as normal or abnormal. It is very time consuming and expensive to manually collect pure normal data and classify data in wireless networks. Good efficiency and performance is obtained with association algorithm and clustering algorithm [1]. The association rule and clustering are used as the root for accompanying anomaly detection of routing and other attacks in MANET.

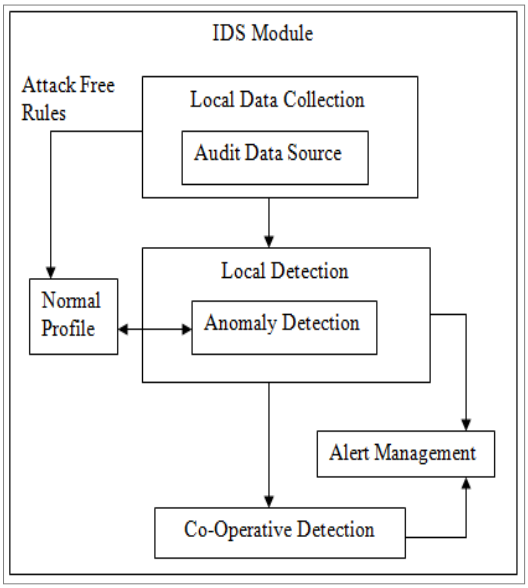

Figure .2: Architecture for IDS

5.2.1. Local Data Collection

The local data collection module collects data streams of various information, traffic patterns and attack traces from physical, MAC and network layers via association module. The data streams can include system, user and mobile node communication activities within the radio range.

5.2.2. Local Detection

The local detection module consists of anomaly detection engine. The local detection module analyzes the local data traces gathered by the local data collection module for evidence of anomalies. A normal profile is an aggregated rule set of multiple training data segments.

New and updated detection rules across ad-hoc networks are obtained from normal profile are recorded. If any detection rules deviate beyond a threshold interval and if it has a very high accuracy rate it can determine independently that the network is under attack and initiates the alert management.

5.2.3 Cooperative Detection

When the support and confidence level is low or intrusion evidence is weak and inconclusive in the detecting node then it can make collaborative decision by gathering intelligence from its surrounding nodes via protected communication channel. The decision of cooperative detection is based on the majority of the voting of the received reports indicating an intrusion or anomaly. The alert management receives the alert from the local detection or co-operative detection depending on the strength of intrusion evidence. It collects them in the alert cache for t seconds. If there are more abnormal predictions than the normal predictions then it is regarded as “abnormal” and with adequate information an alarm is generated to inform that an intrusive activity is in the system.

5.2.4. Alert Management

The alert management receives the alert from the local detection or co-operative detection depending on the strength of intrusion evidence. It collects them in the alert cache for t seconds. If there are more abnormal predictions than the normal predictions then it is regarded as “abnormal” and with adequate information an alarm is generated to inform that an intrusive activity is in the system.

5.3. Combining IDS and Authentication using Data fusion

The figure shows the proposed architecture of the system constituting, an IDS monitoring the systems security state and the multi model biometric Authentication providing the users with the necessary authentication methods to keep the wireless network free from malicious attacks and ensuring security to the MANET. Both IDS and authentication are combined using Data fusion. The below system (Fig. 5.3) implemented only on leaders.

6. DATA FUSION

L sensors are chosen for authentication and intrusion detection [7] 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. It can be quite difficult to ascertain which observers are compromised.

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. The motivation for selecting Dempster–Shafer theory [7] to solve the fusion problem as follows.

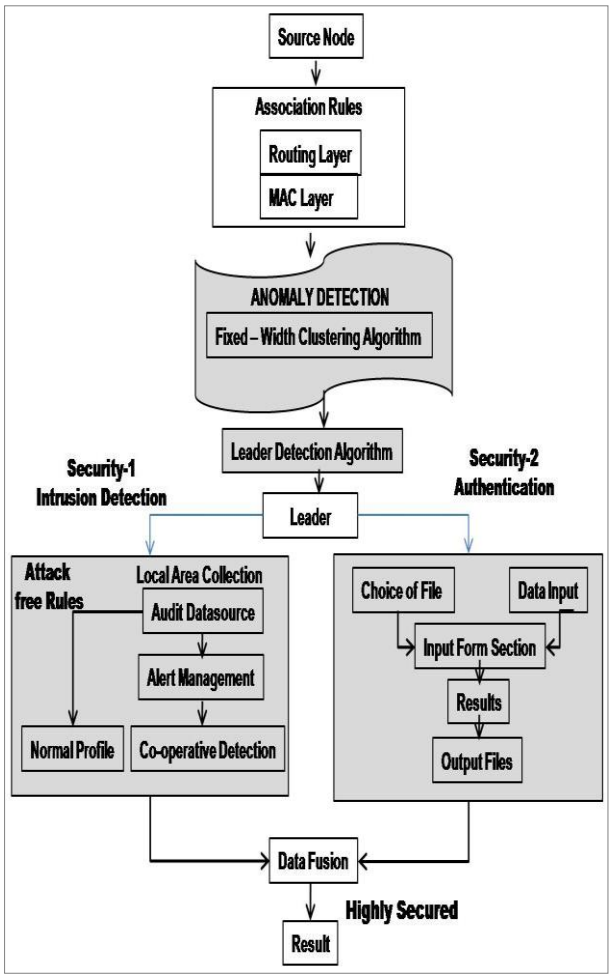

Fig .3: Architecture Diagram

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 [7]. 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 [7]. Note that the theory can be applied for nodes with more than two security states. In this 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* have two security states: 1) Secure state & 2) Compromised state.

7. SIMULATION RESULTS

In this section, the performance of our model with respect to random and connectivity models. We simulate the schemes using Network Simulator 2 (NS2).

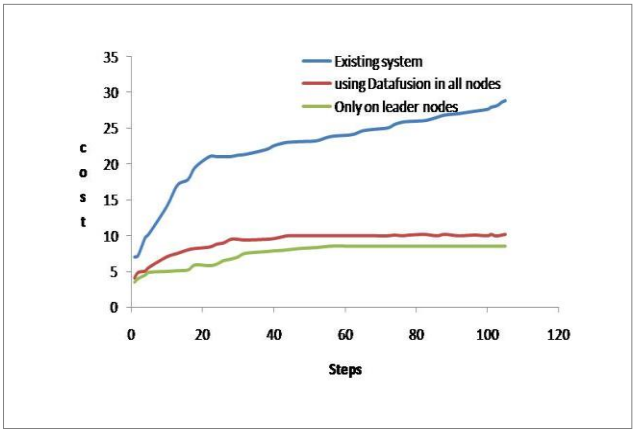

Fig.4: Cost comparison among the proposed scheme with data fusion on leaders, the proposed scheme with data fusion, and the existing scheme.

We run simulations to compare the cost of three approaches: 1) the proposed scheme with data fusion on leaders; 2) the proposed scheme with 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 3000 simulations. Fig. 7.1 shows the average cost for the first 100 steps of the simulation.

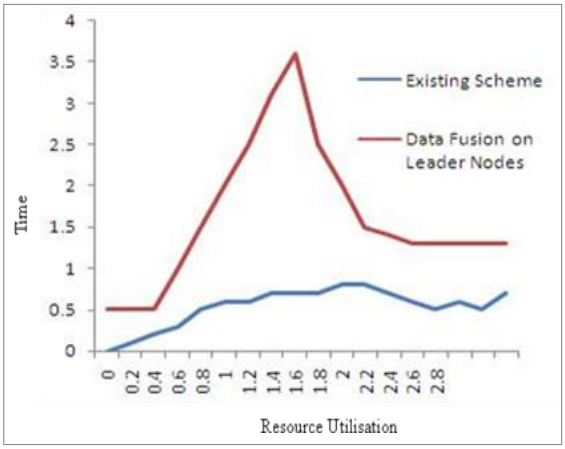

Fig .5: Delay comparison of Existing Scheme and the Proposed Scheme

Simulation is run in two seniors, one with attacker node and another without the attacker node. The below line shows the packets delay between the sources to destination with attacker node. The above line shows packet delay between sources to destination without attacker node. After detecting the intruder fewer packets are delay.

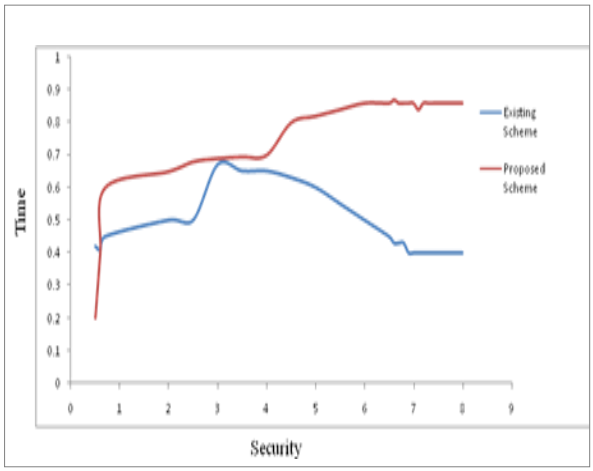

Fig .6: Throughput comparison of Existing Scheme and the Proposed Scheme

Since we combine both IDS and Authentication on Leaders, the performance of the proposed scheme is always better than the existing security system providing higher security to the wireless environment. The existing biometric system is compared with the proposed Intrusion detection and Authentication together combined using the Data Fusion technique on Leaders, so achieving high security in the wireless networks. So the security provided to the MANET is comparatively high and is shown in the performance graph.

8. CONCLUSION

Leader election model and clustering technique in MANET security using Intrusion Detection and Authentication with Data Fusion on Leaders can be an effective approach to improve the security performance in MANETs. In the proposed scheme, the most suitable biosensors for authentication or IDSs are dynamically selected based on the current security posture and energy states. Dempster–Shafer theory has been used for IDS and sensor fusion since more than one device is used at each time slot. 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 used for 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.

9. REFERENCES

[1] Portnoy, L., Eskin, E. And Stolfo, S. (2001), "Intrusion detection with unlabeled data using clustering," in proceedings of the Workshop on Data Mining for Security Applications, November 2001.

[2] Vasudevan, S. DeCleene, B., Immerman, N., Kurose, J. and Towsley, D.(2003), "Leader Election Algorithms for Wireless Ad Hoc Networks," Proc. IEEE DARPA Information Survivability Conf. and Exposition.

[3] Mohammed, N., Otrok, H., Wang, L., Debbabi, M., and Bhattacharya, P. (2008), "A Mechanism Design-Based Multi-Leader Election Scheme for Intrusion Detection in Manets," Proc. IEEE WirelessComm. and Networking Conf. (WCNC).

[4] 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.

[5] 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.

[6] Y. Zhao, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificate less public keys," *IEEE Trans. Dependable Secure Comput.*, vol. 3, no. 4, pp. 386–399, Oct.–Dec. 2006.

[7] 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.

[8] 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.

[9] K.K. Lakshmi Narayanan and A. Fidal Castro, "High Security for Manet Using Authentication and Intrusion Detection with Data Fusion*," International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518*

[10] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi, Seung-Jo Han "A Novel Cross Layer Intrusion Detection System in MANET" *2010 24th IEEE International Conference on Advanced Information Networking and Applications*