ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

An integrated intrusion detection scheme for routing and service level attack discovery

J. Ghayathri[1], L. Parthasarathi[2]

Associate Professor, Department of Computer Science (PG), Kongu Arts and Science College, Erode, Tamil Nadu[1]

Assistant Professor, Department of Computer Science, Sasurie College of Arts & Science, Tirupur, Tamil Nadu[2]

Abstract: Mobile ad-hoc networks are temporary wireless networks. Network resources are abnormally consumed by intruders. Intrusion detection techniques are used for the network attack detection process. The receiver collision, low transmission power and misbehave report authentication attacks are generated in the routing process. The acknowledgement scheme is used to control the routing based attacks. Service level based attacks are raised using service requests. Classification methods are used to discover the service level based attacks. The nodes are grouped into clusters. The leader nodes are assigned for the clusters. Cluster Dependant Leader Election (CDLE) and Cluster Independent Leader Election (CILE) schemes are used in the system. The system optimizes the leader election and intrusion detection process. The system uses the Enhanced Adaptive ACKnowledgment (EAACK) scheme for routing based attack detection process. RSA and Secure Hash Algorithms are used to secure the EAACK scheme. The Bayesian Classification algorithm is used for service level attack detection process. Node mobility is managed by the system.

Keywords: Mobile ad-hoc networks, Intrusion detection, CDLE, CILE, EAACK, Bayesian classification algorithm.

1. INTRODUCTION

1.1 Mobile Ad-hoc Network Basics

Mobile Ad-hoc Network is a peer-to-peer wireless network that it transmits data from computer to computer without the use of a central base station or access point. Routing from one node to another node on mobile ad-hoc networks requires an "on-demand routing protocol," such as Dynamic Source Routing (DSR) or Adaptive On demand Distance Vector (AODV), which generates routing information only when a station initiates a transmission [4]. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet [5].

1.2 MANET Security Issues

There are several key issues and challenges. Some prominent issues and their concepts are described in the following sections.

1.2.1 Link Level Security

In wireless environment the links are susceptible to attacks where eavesdropper can easily spoof the ongoing communication. As there is no protection like firewalls or access control in ad-hoc network any node can become vulnerable to attacks coming from any direction or from any node [9]. The results of such attacks include spoofing of the node's identity, tampering with node's credentials, leaking of confidential information or impersonating node.

1.2.2 Security Factors

To secure an ad-hoc network, consider the following attributes: *availability, confidentiality, integrity, authentication and non-repudiation.*

Availability ensures the survivability of network services despite denial of service attacks.

Confidentiality ensures that certain information is never disclosed to unauthorized entities [3].

Integrity guarantees that a message being transferred is never corrupted.

Authentication enables a node to ensure the identity of the peer node it is communicating with.

Non-repudiation ensures that the origin of a message cannot deny having sent the message.

1.2.3 Key Management

Security goals in ad-hoc networks are achieved through cryptographic mechanisms such as public key encryption or digital signature [2]. These mechanisms are supported through centralized key management where trusted Certificate Authority (CA) provides public key certificate to mobile nodes so nodes can develop mutual trust between one another. Any tampering with CA can easily compromise the security of the entire network.

All proposed solutions require that the mobile users make proper usage of cryptographic keys. Goal of proper management and safekeeping of small number of cryptographic keys is difficult in ad-hoc network due to random mobility of nodes where continuous connectivity is not maintained.

1.2.4 Privacy

Privacy information can be violated by intruders in the mobile ad-hoc networks [8]. The users personal information or network node details can access unauthorized users initiates the privacy violation in the mobile ad-hoc network environment. Spoofing of identity or any confidential information leads to privacy threats and later on that can be engineered to create DoS attacks. Thus privacy is one of the key issues within ad-hoc networking.

1.3 Applications of Mobile Ad-hoc Networks

Mobile ad-hoc networks will most likely be used in cases where there is no fixed wired infrastructure. This may be

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

because it is not economically practical or physically possible to set up the necessary infrastructure, or because the situation does not permit its installation. For example:

- In a conference room during meetings where the participants can share information.
- In a classroom during class discussions/participation with the professor.
- In an airport terminal where coworkers want to share files.
- In an emergency rescue mission among the rescue workers to coordinate the effort.
- In battle among soldiers to coordinate defense or offense.

2. RELATED WORK

2.1 Intrusion Detection Systems

Intrusion detection systems are the 'burglar alarms' of the computer security field. The aim is to defend a system by using a combination of an alarm that sounds whenever the site's security has been compromised and an entity—most often a site security officer (SSO)—that can respond to the alarm and take the appropriate action [6].

In anomaly detection, the system watches abnormalities in the traffic in question. The system takes the attitude which is abnormal and probably suspicious. This detection principle thus flags behavior that is unlikely to originate from the normal process, without regard to actual intrusion scenarios.

In signature detection, the intrusion detection decision is formed on the basis of knowledge of a model of the intrusive process and what traces it ought to leave in the observed system [1].

The detector operates by detecting the intrusion against the background of the normal traffic in the system. The detectors are called as 'signature inspired' because the intrusive model is much stronger and more explicit than the normal model [7].

MANET is a collection of mobile nodes that communicate with each other via bi-directional wireless links either directly or indirectly. There are two types of MANETs, namely single-hop and multi-hop. For single-hop network, nodes are free to directly communicate with other nodes in their radio range [10]. The system uses Enhanced Adaptive ACKnowledgement (EAACK) scheme for intrusion detection process. The main aim of EAACK is to overcome collisions, limited transmission power and false misbehavior, which are three of the major challenges in Watchdog mechanism.

Two techniques were introduced, namely watchdog and pathrater, to detect and mitigate the effects of the routing misbehavior, respectively. The watchdog technique identifies the misbehaving nodes by overhearing on the wireless medium [11]. The pathrater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. The watchdog technique is based on passive overhearing. It can only determine whether or not the next-hop node sends out the data packet.

A leader election algorithm is devised to handle the election process, taking into consideration the possibility of cheating and security flaws, such as replay attack. The algorithm decreases the percentage of leaders, single-node clusters and maximum cluster size and increases average cluster size. The leader performs the route verification and service request verification tasks. Cluster Independent Leader Elimination (CILE) and Cluster Dependant Leader Election (CDLE) schemes are considered in the intrusion detection process. [12].

3. METHODOLOGY

3.1 EAACK Scheme

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK) and misbehavior report authentication (MRA).

ACK scheme is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected.

The S-ACK scheme is an improved version of the TWOACK scheme. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Both DSA and RSA digital signature schemes in there used in the system. The goal is to find the most optimal solution for using digital signature in MANETs.

3.2 Leader Election Schemes

The leader nodes are selected on the basis of coverage information. The leader performs the route verification and service request verification tasks. Cluster Independent Leader Elimination (CILE) and Cluster Dependant Leader Election (CDLE) schemes are considered in the intrusion detection process.

In CILE, each node must be monitored by a leader node that will analyze the packets for other ordinary nodes. Based on the cost of analysis vector C, nodes will cooperate to elect a set of leader nodes that will be able to analyze the traffic across the whole network and handle the monitoring process. The mechanism provides payments to the elected leaders for serving others. The payment is in the form of reputations, which are then used to allocate the leader's sampling budget for each node.

In CDLE, the whole network is divided into a set of clusters where a set of 1-hop neighbor nodes forms a

DOI 10.17148/IJARCCE.2015.4250

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

cluster. The scheme is used to cluster the nodes into 1-hop clusters. Each cluster then independently elects a leader among all the nodes to handle the monitoring process based on nodes' analysis cost. The objective is to find the most cost-efficient set of leaders that handle the detection process for the whole network.

3.3 Naive Bayes Classification Algorithm

The Naïve Bayes classifier algorithm is used to detect the intruders under the MANET environment. The classification algorithm analyzes the network traffic data. Attack types are discovered by the algorithm using the anomaly based analysis mechanism. The classification algorithm is divided into two parts, they are learning phase and testing phase. The learning phase is used to learn attack patterns. The testing phase is applied to discover the attacks using the learned patterns

– **Learning Phase**:
– Begin
• Given a training set **S**,
• For each target value of c_i (c_i = c_1,…….,c_l)
• $\hat{P}$ (C=c_i)← estimate P(C=C_i) with examples in S;
• For every feature value x_{jk} of each feature (j=1,….,n, k=1, ….., N_j)
• $\hat{P}$(X_j=x_{jk}|C=c_i) ← estimate P(X_j=x_{jk}|C=c_i) with examples in S;
• Output conditional probability tables; for X_j, N_j × L elements
– End
– **Test Phase**:
– Begin
– Given an unknown instance X'=(d_1,……d_n)
– Look up tables to assign the label *c** to **X'** if
– $[\hat{P}(a_1^t|c^*) \ldots\ldots \hat{P}(a_n^t|c^*)]\hat{P}(c^*) > [\hat{P}(a_l^t|c\ \ ) \ldots\ldots \hat{P}(a_n^t|c)\hat{P}(c), c \neq c', c = c_1, \ldots\ldots, c_1$
– Output Label for transactions
– End

3.4 RSA Algorithm

The domain name service sensitive attributes are secured using the RSA algorithm. The Rivert, Shamir, Adelman (RSA) scheme is a block cipher in which the Plaintext and cipher text are integers between 0 and n-1 for some n.

Key Generation

Select p,q p and q both prime , p≠q
Calculate n = p x q
Calculate $\phi(n)=(p-1)(q-1)$
Select integer e gcd($\phi(n)$,e) = 1; 1 <e < $\phi(n)$
Calculate d $d = e^{-1} \bmod \phi(n)$
Public key KU = {e, n}
Private key KR = {d, n}

Encryption

Plaintext M <n
Cipher text $C = M^e \pmod n$

Decryption

Cipher text C
Plaintext $M = C^d \pmod n$

3.5 SHA1 Procedure

In cryptography, Secure Hash Algorithm-1 is a cryptographic hash function. SHA-1 produces a 160-bit (20-byte) hash value. A SHA-1 hash value is typically expressed as a hexadecimal number, 40 digits long. The four SHA algorithms are structured differently and are distinguished as *SHA-0*, *SHA-1*, *SHA-2* and *SHA-3*.

4. RESULTS AND ANALYSIS

The secure leader election and intrusion detection system is tested under the simulation environment. The mobile ad-hoc network construction and cluster formation operations are tested under the simulation environment. The network and node parameters are collected from the users. The mobile ad-hoc network is constructed with reference to the user specifications. The node movement and packet transmission process are initiated by the simulation environment automatically. The EAACK scheme and Bayesian network based classification model are used in the intrusion detection process.

The EAACK scheme is assigned to manage routing related attacks. The Bayesian classification scheme is used to handle service request level based attacks. The system uses two types of detector assignment methods. They are cluster based detector assignment (CDA) and Cluster Integrated Detector Assignment (CIDA) methods. In the cluster based model the detectors are assigned under the leader nodes of all clusters. In the cluster integrated model the detectors are assigned for a group up clusters. The detector count is reduced in the cluster integrated model. The energy consumption and traffic rate performance metrics are used to evaluate the system performance.

4.1 Performance Analysis

4.1.1 Energy Consumption

The energy consumption analysis is performed with different node count levels. The system is tested with CDA and CIDA model with energy usage levels. The energy usage of each node is calculated then the average energy level for the entire network is estimated. The average energy usage analyzed for the CDA and CIDA models. The CIDA model reduces the energy consumption 10% more than CDA model.

Nodes	CDA	CIDA
20	81.3	69.8
40	84.6	72.1
60	87.4	75.6
80	91.3	79.2
100	94.8	81.4

Table 1. Energy consumption analysis between CDA and CIDA

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

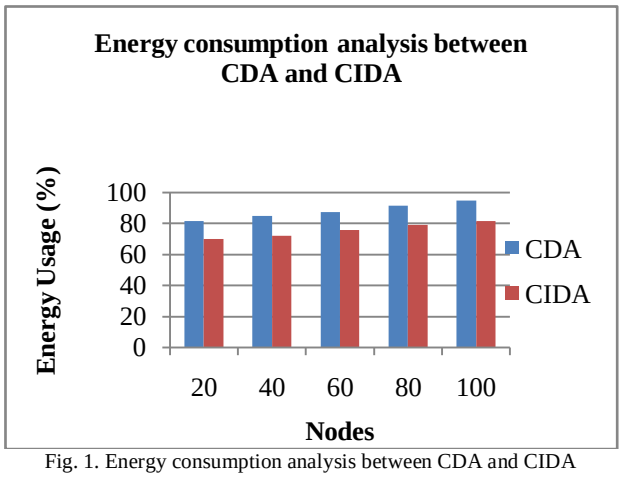

Fig. 1. Energy consumption analysis between CDA and CIDA

4.1.2 Traffic Rate

The traffic rate analysis is performed to measure the bandwidth usage level for the mobile ad-hoc network. The traffic analysis is performed with reference to the system message transmission process. The traffic rate analysis is performed with CDA and CIDA models. The CIDA model reduces the traffic rate 15% more than the CDA model.

Nodes	CDA	CIDA
20	75.8	57.4
40	79.2	59.7
60	83.6	62.1
80	85.9	65.8
100	89.1	68.5

Table 2. Traffic Rate analysis between CDA and CIDA

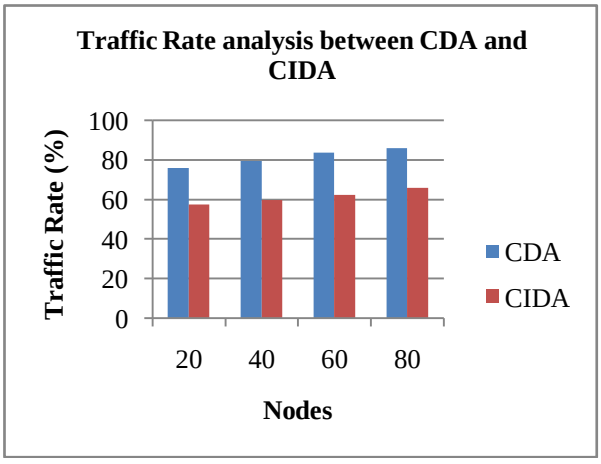

Fig. 2. Traffic Rate analysis between CDA and CIDA

4.1.3 Detection Latency

The detection latency is analyzed for the intrusion detection process. The detection period for attack detection is measured in all detectors. The average detection period is measured as detection latency for the entire network.

Nodes	CDA	CIDA
20	11.2	10.1
40	11.5	10.5
60	11.9	10.4
80	12.2	10.8
100	12.4	10.9

Table 3. Latency Analysis between CDA and CIDA

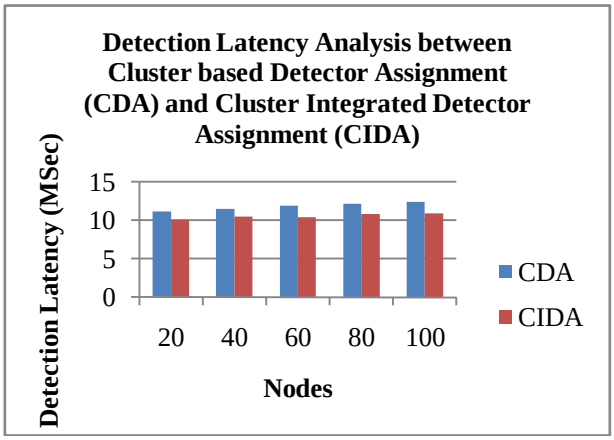

Fig. 3. Detection Latency Analysis between CDA and CIDA

5. CONCLUSION & FUTURE ENHANCEMENT

5.1 Conclusion

The mobile ad-hoc networks are infrastructure less environment. The system performs two types of intrusion detection process. The routing based attack detection process uses the EAACK scheme. RSA algorithm and Secure Hash Algorithm (SHA) are used for the security process. The service request based attack detection is integrated with the system.

The EAACK scheme is used for the routing level attack detection process. The Bayesian classification algorithm is used for the service request based attack detection process. The cluster based detector assignment model and cluster integrated detector assignment models are used for the detector assignment process.

The simulation process is tested with different network conditions and node count levels. The energy consumption, traffic rate and detection latency performance metrics are used to evaluate the system performance. Dynamic interval is assigned for intrusion detection process. The system reduces energy consumption, network traffic and detection latency in all network conditions.

5.2 Future Enhancement

The mobile ad-hoc network intrusion detection system is development to handle attack detection on routing process and service request process. The system can be enhanced with the following features.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

- The signature based model can be integrated with the system to improve the accuracy levels.
- The system can be adapted for the wireless mesh network environment.
- The system can be adapted for the shared service management process to support service discovery operations.
- The current intrusion detection system uses the anomaly based technique for the intrusion detection process.
- The system can be integrated with multicast routing schemes.

REFERENCES

[1]. Ben Hammond, "Digital Signatures", Publisher: McGraw-Hill Professional, February 8, 2002.
[2]. Jonathan Katz, "Digital Signatures (Advances in Information Security)", Publisher: Springer; 1st Edition, May 15, 2010.
[3]. Scott Urman Steve Rackley, "Wireless Networking Technology: From principles to successful implementation", Publisher: Newnes, 2007.
[4]. Bulent Tavli and Wendi Heinzelman, "Mobile Computing" Springer; 1 edition 2006.
[5]. Ron Hardman and Michael McLaughlin "Oracle Database 10g PL/SQL Programming", Publisher: McGraw-Hill Osborne Media; 1st edition, 2004.
[6]. Wenbo Mao "Modern IDS: Theory and Practice" Publisher: Prentice Hall PTR; 1st edition 2003.
[7]. Whiztoolsm "Digital Signature Creator", Publisher: McGraw-Hill Professional, 2013.
[8]. Bin Tang, Baoliu Ye and Dapeng Oliver Wu, "Order-Optimal Information Dissemination in MANETs via Network Coding", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 7, July 2014.
[9]. Chunxiao Cai, Yueming Cai and Wendong Yang, "When Does Relay Transmission Give a More Secure Connection in Wireless Ad Hoc Networks?", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014.
[10]. Nan Kang, Elhadi M. Shakshuki and Tarek R. Sheltami, "Detecting Misbehaving Nodes in MANETs", 2009.
[11]. https://www.uncg.edu/cmp/faculty/j_deng/papers/2ack_tomc06.pdf.
[12]. https://www.it.ecei.tohoku.ac.jp/pdf-nopass/journal-papers/2012-TPDS-wei.pdf.

BIOGRAPHIES

J. Ghayathri is currently working as Associate Professor in Computer Science (PG), Kongu Arts and Science College, Erode. Tamil Nadu, India.

L. Parthasarathi is currently working as Assistant Professor in Computer Science, Sasurie College of Arts & Science, Tirupur. Tamil Nadu, India.

DOI 10.17148/IJARCCE.2015.4250