British Journal of Mathematics & Computer Science
7(1): 26-39, 2015, Article no.BJMCS.2015.100
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Incorporation of 3-phase Commit Protocol into the Existing Intrusion Detection Systems in the Mobile Ad-hoc Network

Makanjuola Daniel[1*]

[1]Department of Computer Science, Salem University, Lokoja, Kogi State, Nigeria.

Article Information

DOI: 10.9734/BJMCS/2015/14987
Editor(s):
(1) Doina Bein, Applied Research Laboratory, The Pennsylvania State University, USA.
(2) Paul Bracken, Department of Mathematics, The University of Texas-Pan American Edinburg, USA.
Reviewers:
(1) Anonymous, India.
(2) Anonymous, Romania.
(3) Anonymous, USA.
(4) Anonymous, India.
(5) Anonymous, Nigeria
Complete Peer review History: http://www.sciencedomain.org/review-history.php?iid=932&id=6&aid=7953

Original Research Article

Received: 31 October 2014
Accepted: 24 December 2014
Published: 30 January 2015

Abstract

A mobile ad-hoc network is a collection of mobiles nodes forming an ad-hoc network without the assistance of any centralized structures [1]. It is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in mobile ad-hoc network themselves are responsible for dynamically discovering other nodes to communicate.

As a result of certain unique properties in mobile ad-hoc networks, the on-going trends in the communication industries is advancing towards the adoption of ad-hoc networks for commercial and security issues. This subsequently exposes mobile ad-hoc networks to various external attacks from un-authorized bodies. This paper is segmented into various sections; the first section introduces the reader to the concept of MANETs and gives account of its level of vulnerability to intruders' attack; the second section addresses sources of threats posed to wireless network, the threat involved, the types and effects of threats. In the same line of progression, comprehensive details were given on statement of problems with special focus on the weakness on the existing researches in respect to improving security on mobile ad-hoc networks. Further, the content of the paper explains the motivation of study and later sheds light on the research objectives. Subsequently, details were given on the significance of study; that is, the dividends of this research on various application areas. The next section makes an explicit highlight about the existing models of Intrusion Detection Systems (IDS), giving a concise account of their area of strengths and weaknesses. The tail end of the paper introduces the working concept of a 3-phase commit protocol and how this concept was modeled to stand

**Corresponding author: danielmakanjuola@salemuniversity.edu.ng;*

as a three in one intrusion detection systems algorithm, integrating the functionalities of the three notable existing intrusion detection systems (IDS): CONFIDANT, OCEAN and CORE. Subsequently, I describe the implementation concept of IIDSA, giving rational for picking on 3-phase commit protocol as a viable instrument in its plight to sieve out malicious nodes in a multi-user network.

Keywords: IIDSA; MANETS; Transaction.

1 Introduction

The modern trends of networking have witnessed a complete shift in taste from wired infrastructures to wireless networks. Personal Computer (PC) sales continue to trend towards more laptop sales versus desktop computers, in part to support a more mobile work-force. PC users need to connect to whatever network they are near, whether at work, at home, in a hotel, or at a coffee shop. The migration towards a work model in which the user finds working moments wherever he finds himself with a need to be connected to an organization network through the internet conceives the phenomenon called Mobile ad-hoc network (*MANET*). Although security has been an active research topic in wired networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. As stated by Rakesh et al. [2], some of the factors associated with MANETs which make it more vulnerable than wired network include but not limited to the following:

i. Open network architecture
ii. Shared wireless medium
iii. Stringent resource constraints
iv. Highly dynamic network topology

The ultimate goal of the security solutions for MANETs is to provide security services that would alleviate (if not completely eliminate) the threats posed by intruders. Several techniques and algorithms have been employed, part of which are CORE (A Collaborative Reputation Mechanism to enforce node cooperation in mobile ad-hoc networks) [3], OCEAN (Observation-based Cooperation Enforcement in Ad-hoc Networks) [4] and CONFIDANT [5]. Despite the implementation of these notable algorithms, hackers still persist in perpetuating havoc within mobile ad-hoc networks (MANETs). In the light of this, an algorithm that implements interoperability of these commonly known security concepts (i.e OCEAN, CORE and CONFIDANT) was designed. It is called Integrated Intrusion Detection System Algorithm (IIDSA). IIDSA combines the functionalities and security concepts inherited in OCEAN, CORE AND CONFIDANT, employing the working mechanism of 3-phase commit protocol [11] to track the potential malicious nodes in the wireless network. IIDSA makes the task of cracking into an organization network a tedious adventure for malicious and illegitimate staff.

1.1 Sources of Threats in the Mobile Ad-hoc Networks (MANETS)

According to [6], threats to security as it relates to agent systems are generally classified into three main classes;

i. Disclosure of Information
ii. Denial of Service (DoS)
iii. Corruption of Information

In the study undertaken by Wayne and Tom [6], components of an agent system are used to categorize the threats as a way to identify the possible source of attack. For instance, the agent system model developed by [6], reflects that possible threats may arise from agent-to-agent platform interaction, agent platform-to-agent interaction or agent attacking another agent's platform.

The style of attack under each category may be similar by way of approach but different in context. For instance, all the highlighted threat categories enumerated in [6] possess similar approaches like Masquerading, Denial of Service and Unauthorized access but the pattern of attack under each platform differs.

Masquerading in agent-to-agent platform context illustrates a scenario whereby unauthorized agents claim the identity of another agent with a view to gaining access to the services and resources of a platform to which it is not entitled whereas masquerading in agent-to-agent interaction is when an agent attempts to hide its identity in an effort to deceive another agent of the same platform with which it is communicating.

Furthermore, Denial of Service (DoS) in platform-to-agent approach of attack is entirely different to what and how it is perpetuated on other-to-agent platform. Platform-to-agent approach details its version of DoS as a new agent arrives on a platform, having completed a transaction, expecting the platform to process its business request appropriately, provide fair allocation of network resources and abide by quality of service agreement, but the platform goes the other way around and ignore agent service request, introduce unacceptable delays for critical tasks or simply not execute the agent's code.

On other-to-agent platform however, the DoS attack comes up as the agent services offered by the agent platform is disrupted with a view to underlying operating system and generate a bottleneck among the communication protocols during inter-platform transactions by other entities accessing the platform from a remote locations.

1.1.1 Other categories of threats include

Repudiation (Agent-to-Agent)
Eavesdropping (Agent Platform-to-Agent)
Alteration (Agent Platform-to-Agent)
Copy and Replay (Other-to- Agent Platform)

1.2 Statement of Problems

The first security scheme provided by IEEE 802.11 standards is called Wired Equivalent Privacy (WEP) in 1997. Basically, it was designed to provide security for wireless local area network (WLAN). But it suffers from many design flaws and some weaknesses in the way RC4 cipher is used in Wired Equivalent Privacy. It is well known that WEP is vulnerable to message privacy and message security attacks and probabilistic cipher key recovery attacks. Later, WEP was replaced by Advanced Encryption Standard (AES) in *IEEE 802.11i***.** Some of the weaknesses of the WEP are described below:

i. Key management is not specified in the WEP protocol. Lack of key management is a potential exposure for most attacks exploiting manually distributed secrets shared by large populations.
ii. The initialization vector (*iv*) used in WEP is a 24-bit field which is sent in clear and is a part of the RC4 that leads to probabilistic cipher key recovery attack or most commonly known as analytical attack
iii. The combined use of a non-cryptographic integrity algorithm CRC 32 with the stream chipper is a security risk and may cause message privacy and message integrity attacks.

The above listed points enumerate some of the problems inherited in (WEP). However, there are some modifications to WEP like CISCO solution (in 2001) called WI-FI Protected Access (WPA, 2003) and (WPA, 2006) [7]. Despite the con-current solution to mobile a-hoc network, hackers still persisted at hacking into the medium to cause havoc. This paper is inclined to address those lapses and develop algorithm that sees to alleviate the threat involved. IIDSA is an algorithm inclined to harmonize the activities of a 'real-time' web-based client/server application system in an

interactive manner such that before any transaction could be committed, some trends of communication must be acknowledged between the clients and the server. This is made obligatory to sieve out any malicious client (node) who may be smart at predicting the consensus of the legitimate clients in the network.

1.3 Motivation of Study

As mobile ad-hoc network is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. A secure communication medium enables a smooth data flow which in turn strengthens the interoperability of various nodes or devices involved in the organizations. There are quite a number of promising qualities that could be derived from a well secured mobile ad-hoc network.

For instance, the military can track an empty tank as it moves through the geographic area covered by the network when there is a smooth and secured transmission of data from one wireless station to another.

Secondly, metropolitan traffic warder using mobile devices can use ad-hoc network to detect an over speeding car moving through an intersection, checking the speed and direction of the car. Furthermore, in an environment network, where all nodes are securely connected, one can find out a metrological profile of a particular environment like temperature, atmospheric pressure, amount of sun-light, and the relative humidity at a number of locations. Aviation industries also makes use of a mobile devices called radar in the aircraft to contact the next available tower building and ensure safe landing. In a situation where the tower building has been intercepted, a terrorist can easily send a false signal to the pilot. This could expensively lead to a crash-landing and ultimately result in the loss of innocent lives.

1.4 Aim and Objectives of Study

The aim of this research is to design and develop an algorithm that combines the functionalities of the three notable models of intrusion detection systems; notably, CONFIDANT, OCEAN and CORE, mimicking the working concepts of 3-phase commit protocol. However, it is in line with the objectives of this publication to buttress the following facts in the mobile ad-hoc network:

i. Intimate the reader about the existing threats on a mobile ad-hoc network.
ii. The effect of each category of threat.
iii. The existing models of intrusion detection system (IDS) - CONFIDANT, OCEAN and CORE.
iv. A notable working concept of computing called 3-phase commit protocol and its simulation to function as an intrusion detection system that integrates the functionalities of CONFIDANT, OCEAN and CORE.

1.5 The Significance of Research

At the end of this research, it is believed that the proposed algorithm would be well-suited to checkmates various threats posed to the mobile ad-hoc network as well as other mobile devices. A clear and smooth transmission of signals can significantly contribute to the overall performance of various networks that deal with exchange of information using mobile devices.

A secure distributed network serves to influence various organizations which include the following:

i. Ministry of Aviation
ii. Ministry of Defense (Air-force, Naval and Armed forces)

iii. Metrological stations
iv. Ministry of Communication Technology
v. Metropolitan Police Force
vi. Universities and various Research Industries

1.6 Existing Models of Intrusion Detection Systems

1.6.1 First model of intrusion detection system – CONFIDANT

CONFIDANT, detects misbehaving nodes by means of observation or by alarm signals from the neighborhood [5]. CONFIDANT aggressively informs nodes in the neighborhood about the misbehaving of a malicious node.

The weight-age of ALARM warning signals depends upon the level of trust that is believed by the receiving node. Each ad-hoc network running a CONFIDANT system comprises of the following:

i. *Monitor*- for observation purposes
ii. *Reputation Manager* – for calculating reputation of other nodes
iii. *Trust Manager* – for calculating level of trust to a particular node, which is used in calculating weight-age of ALARM from that node
iv. *Path Manager* – for updating path information in route cache as the reputation of neighborhood nodes changes. For Example, deletion of paths containing malicious node, selection of path from various available paths option on a particular situation and so forth

CONFIDANT is vulnerable to false accusation if trusted nodes lie or if several liars collude.

1.6.2 Second model of intrusion detection system – CORE

Michiardi and Molva [3] proposed a mechanism called CORE, A collaborative reputation mechanism to enforce node cooperation in mobile ad-hoc networks. In this mechanism, reputation is a measure of participating nodes' contribution to network operations. Members that have a good reputation can use available resources, while members with a bad reputation, because they refuse to cooperate, are gradually evicted from the community.

CORE defines three types of reputation:

Subjective Reputation: This is a reputation value which is locally calculated based on direct observation
Indirect Observation: This is secondhand reputation information which is established by other nodes
Functional Reputation: This is related to a certain function, where each function is given a weight as to its importance. For example, data packet forwarding may be deemed to be more important than forwarding packets with route information, so data packet forwarding will be given greater weight in the reputation calculations.
Problems of CORE: CORE reputation values range from positive (+1), through null (0), to negative (-1). CORE suffers from the problem of unwanted consequence of good reputation, where a good node may even wish to decrease its reputation by behaving badly to prevent its resources from being overused. The CORE mechanism assumes that every node will use the same reputation calculations and will also assign the same weight to the same functions. This is a potentially inappropriate assumption in heterogeneous ad-hoc networks, where devices with different capabilities and roles are likely to place different levels if importance on different functions depending upon the processor usage, battery usage and so forth. One can take advantage of this situation and may perform only those functions which have higher preferences in calculating reputation.

1.6.3 Third model of intrusion detection system – OCEAN

Another type of intrusion detection system is one that solely depends upon the firsthand observation for reputation maintenance. It is referred to as OCEAN "Observation-based Cooperation Enforcement in Ad-hoc Network". Nodes make routing decision based on only the direct observation of its neighbor's node. This eliminates most of the trust manager complexity. In highly mobile ad-hoc network, it might not be appropriate to only depend solely upon personal observation, but also using secondhand information can significantly accelerate the detection and subsequently isolation of malicious nodes in mobile ad-hoc networks.

OCEAN by Bansal and Baker [4] relies exclusively on firsthand observations for rating and avoids indirect (secondhand) reputation information. In OCEAN, the rating of each node is initialized to neutral (0), with every positive action resulting in an increment (+1) of the rating, and every negative action resulting in a decrement (-2) of the rating. Once the rating of a node falls below a certain faulty threshold (-40), the node is evicted and added to a faulty list. The faulty list represents a list of misbehaving nodes.

If the rating is below the faulty threshold, the node is added to the faulty list. This faulty list is appended to the route request by each node, broadcasting it to be used as an avoid list. A route is rated good or bad depending on whether the next hop is on the faulty list. In addition to the rating, nodes keep track of the forwarding balance with their neighbors by maintaining a chip count for each node.

OCEAN's approach is to disallow any secondhand reputation exchanges. Routing decisions are made based solely on direct observations of neighboring nodes behavior. This eliminates mostly, the trust management complexity. The basic problem with OCEAN is that it does not take secondhand information that can significantly improve detection of malicious nodes. Also, authors only consider an individual's bad behavior, not collusion of nodes.

1.7 Commit Protocols

Commit Protocols (CP) are distributed algorithms that guarantee the atomic property of transactions. Commit protocol ensures that all databases in the multi-user environment have the same understanding, which is clear and true to every node involved. All the nodes by rule are enforced to perform the same operations either to commit or abort a particular transaction in a multi-user environment [8].

If a transaction fails, then the commit protocol rolls back, guaranteeing that any change made to any of the component databases are removed from those databases [8]. The 3-phase commit protocol concept needs to be implemented in the intrusion detection systems as a result of the weaknesses in the existing intrusion detection systems (i.e, CONFIDANT and CORE).

1.7.1 Three-phase commit protocol

The three phase commit protocol is a non-blocking protocol. Blocking occurs in a network, when some participants have voted and other participants are indecisive about their voting status. Specifically, blocking takes place when the resources of nodes that have already voted are held ransomed for a long time. However, a three phase commit protocol solves blocking problem where a network is not partitioned [9].

The three phase commit protocol is to remove the uncertainty period for participants who have "COMMIT", and are waiting for the coordinator's decision. It is an upgraded version of 2-phase commit protocol. Three phase-commit protocol introduces a third phase called "PRE-COMMIT" between the voting nodes and the coordinator's decision.

On receiving all votes from the participants, the coordinator sends a PRE-COMMIT message. A participant who receives a PRE-COMMIT message knows that all participants have voted "COMMIT" message. All nodes then executes commit on the transaction, and sends acknowledgement message back to the coordinator [10].

Fig. 1, below shows the mode of operations of a 3-phase commit protocol on a commit transaction. A node is designated as the coordinator that coordinates all the activities. To enforce atomicity, all nodes notify the coordinator about their interest on a particular transaction. The coordinator instructs all nodes to vote and coordinates the voting activities among the nodes. At the end of the voting activities, if all the nodes agree to commit the transaction, the coordinator sends a prepare to commit (PRE-COMMIT) notification to all nodes which act accordingly and send a "ready to commit" message back to the coordinator. The coordinator then sends a "COMMIT" message to all nodes. Each node executes the "COMMIT" instruction, updates their routing table and sends an acknowledgement message back to the coordinator who also updates its own routing table, thus making all the transactions to be in a consistent state.

1.7.2 Mode of operation of 3-phase commit protocol

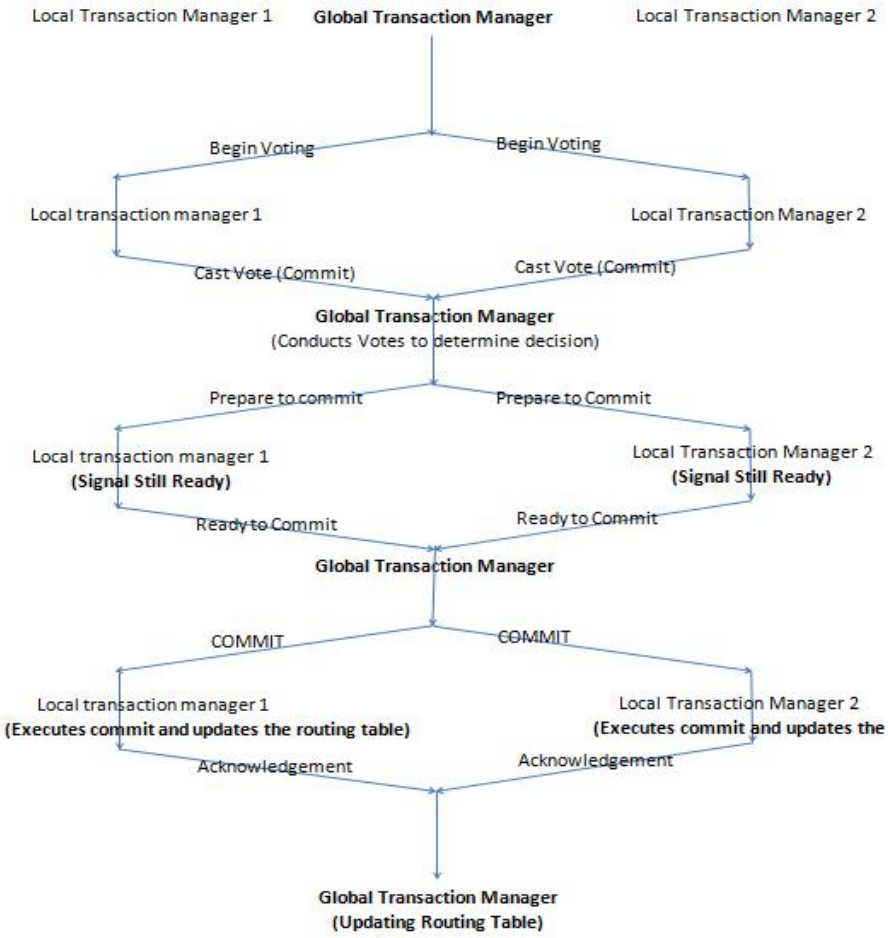
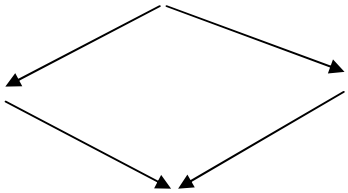


Fig. 1. A Commit transaction

Notable Key in the Fig. 1:

The two upper arrows pointing downward signify instruction from the Global Transaction Manager to the Local Transaction Managers



The two lower arrows signify the response from the Local transaction Managers to the Global Transaction Manager

Fig. 2 below shows the mode of operation of a 3-phase commit protocol for an "*abort*" transaction. The most trusted node is designated as the coordinator that coordinates all the activities going on within the network. In an effort to enforce atomicity, all nodes notify the coordinator about their interest on a particular transaction. The coordinator instructs all nodes to vote and coordinates the voting activities among all the nodes. At the end of the voting activity, if one or more nodes abort, the coordinator sends a "*prepare to abort*" notification to all nodes which acts accordingly. All nodes then send a "*ready to abort*" message back to the coordinator. The coordinator then sends an "*abort*" message to all nodes. Each node executes the abort instruction, updates its routing table and sends an acknowledge message back to the coordinator who also updates its own routing table, thus ensuring that all the databases are in consistent state.

1.7.3 Mode of operation of 3-phase abort protocol

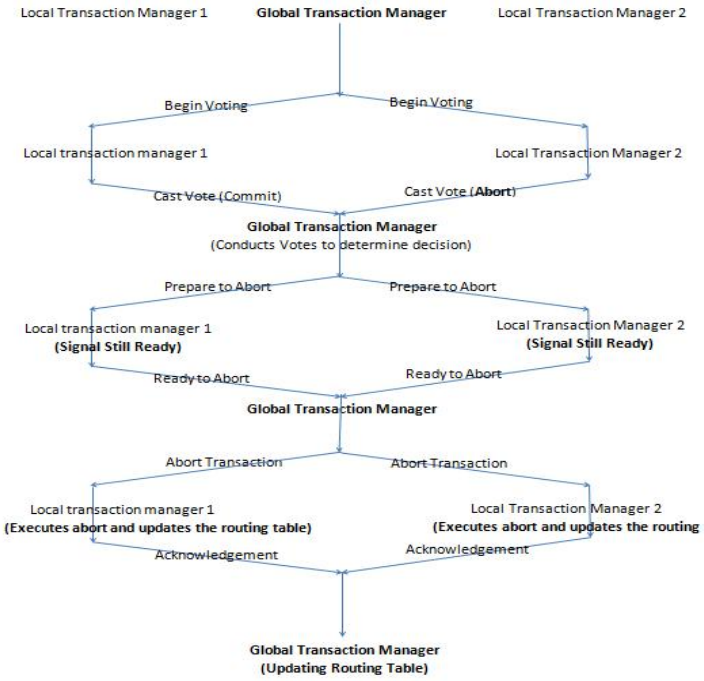
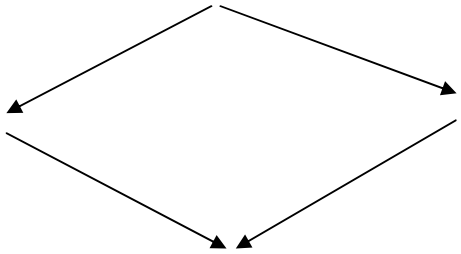


Fig. 2. An abort transaction

Notable Key in the Fig. 2:

The two upper arrows pointing downward signify instruction from the Global Transaction Manager to the Local Transaction Managers



The two lower arrows signify the response from the Local transaction Managers to the Global Transaction Manager

1.8 Mode of Operation of the Proposed Model on Intrusion Detection Systems Algorithm

When a node suspects a misbehaving node in the network, it notifies the coordinator. The coordinator solicits the view of other nodes within the network by sending a voting instruction. The vote about the alleged malicious node will be based on their first-hand or personal experience with the suspected node.

At the end of the votes, if the majority agrees that the node is malicious based on the vote result, the suspected node will be convicted and all other nodes shall erase the route associated to that malicious node from their routing table.

Having disengaged the malicious node from the network, the remaining nodes will send acknowledgement messages together with their new updates to their coordinator who will make replicated copies about the position of each node's updates in the network.

On the other hand, if the vote result signifies that the node alleged to have been malicious is not guilty of the accusation, the coordinator will instruct all nodes to ignore the notification, tagging it as a false alarm. Accordingly, all nodes will also send acknowledgement message to the coordinator.

1.9 Incorporation of 3-phase Commit Protocols Concept into Intrusion Detection System (IDS) – Design Model

The work pattern of 3-phase Commit Protocol was adapted into the mode of operation of the intrusion detection systems (IDS). Our proposed model will work in accordance to the following format;

i. Just like CORE Intrusion Detection System (IDS), the level of trust on each node will be based on the level of supportive contribution of each node in the network.
ii. Each node will keep private account of its experience with all other nodes, either they perform as expected or they act maliciously.
iii. The level of trust of each node will be based on the number of successful contributions to the flow of data packets in the network.
iv. The most trusted node in this regard will be designated as the coordinator who will oversee all activities that take place within the network.

v. Also, as in CONFIDANT (IDS) model, each node in the network is empowered to raise alarm on any suspected malicious node.

Fig. 3, shows the mode of operation of the proposed model of the improved intrusion detection system algorithm for a genuine node using the three phase commit protocol.

1.9.1 Mode of operation of the improved intrusion detection system algorithm (IIDSA)

When a node notices a malicious behavior of a particular node in the network, it sends alarm to the global coordinator about the misdeeds. The coordinator receives the alarm and seeks the opinions of all nodes by conducting votes among all nodes within the network. If the result by majority votes vindicates the alleged node as being genuine, the coordinator sends a "*prepare to exonerate*" message to all the nodes which acts accordingly and then sends a "*ready to exonerate*" reply back to the coordinator. The coordinator then sends an "*exonerate*" message to all the nodes to ignore the alarm, tagging it as a false negative. All nodes exonerate the node as innocent and continue their transactions with the node as displayed in Fig. 3 below.

Mode of Operation of the Improved Intrusion Detection System Algorithm (IIDSA)

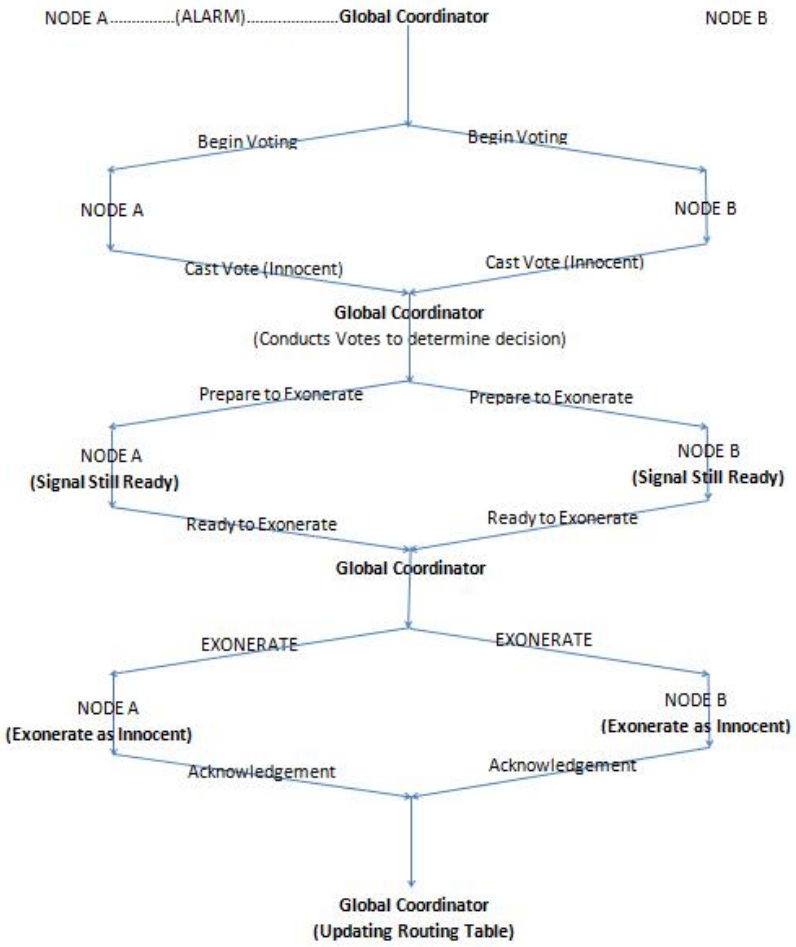
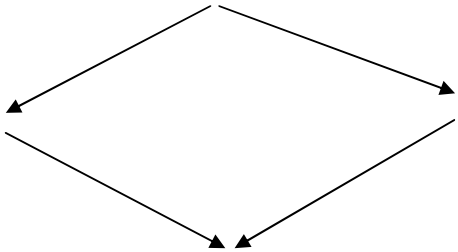


Fig. 3. A vindicated node

Notable Key in the Fig. 3:

The two upper arrows pointing downward signify instruction from the Global Coordinator to the Nodes



The two lower arrows signify the response from the Nodes (Clients) to the Global Coordinator

Furthermore, Fig. 4 gives the analysis of what takes place in the event of a convicted node, displaying the mode of operation of (IIDSA) for a malicious node using the three phase commit protocol.

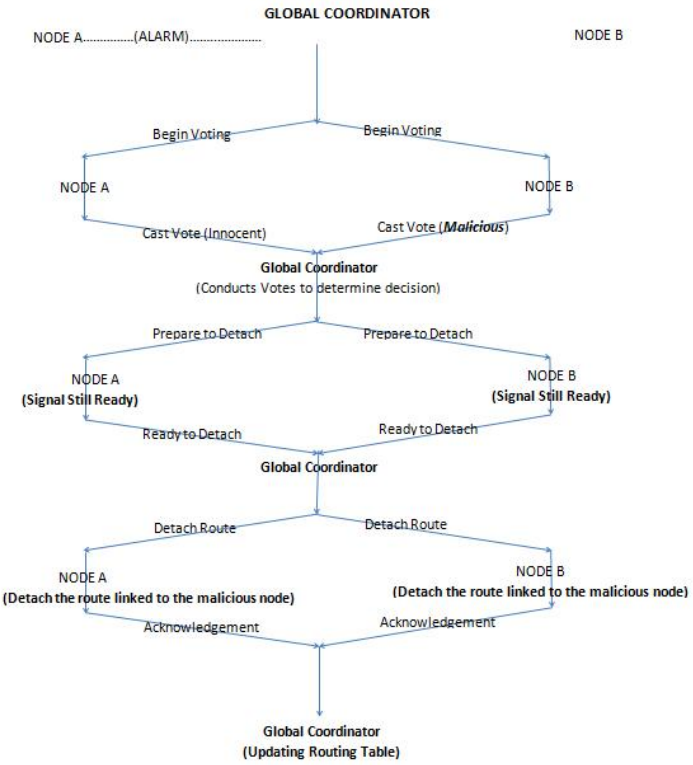
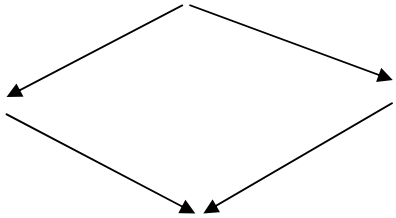


Fig. 4. A convicted node

Notable Key in the Fig. 4.

The two upper arrows pointing downward signify instruction from the Global Coordinator to the Nodes



The two lower arrows signify the response from the Nodes (Clients) to their Global Coordinator.

When a node notices a malicious behavior of a particular node in the network, it sends alarm to the global coordinator about the malicious misdeeds. The coordinator receives the alarm and seeks the opinions of all the nodes by conducting votes among all nodes within the network. If the result of the majority votes convicts the alleged node as malicious, the coordinator sends a "*prepare to detach*" message to all nodes which act accordingly. All nodes then send a "*ready to detach*" reply back to the coordinator. The coordinator sends a "*detach route*" message to all the nodes to detach the route associated with the node from the routing table. Each node detaches the route linked to the malicious node from its routing table and sends an update of the current status of its routing table to the coordinator.

1.9.2 Real-time application of IIDSA

IIDSA is designed for use on web-based client/server application systems (R/3 Systems) where efficient and safe communication of data objects is necessary for inter-transactions between the entities that make up the system. In R/3 systems, workflow (business processes) is modeled using user-defined EPC (Event-control Process Chain) [11]. I believe that if IIDSA is integrated to R/3 systems or any other web-based client/server application system, it would go a long way in check mating malicious activities as hackers or intruders would not be able to get correctly the series of communication as displayed by IIDSA before a sequence of database operations could be committed.

1.9.3 The basic reasons for adopting 3-phase commit protocols

i. In CONFIDANT, malicious node often makes unfair remarks about legitimate nodes which mostly lead to a removal of legitimate nodes from the network.
ii. In CORE, the trusted node attracts much interests and interactions from other nodes and as such, most of their resources are being delegated for accomplishing other nodes' tasks in the network. The much interests and interactions to the resources of the trusted nodes sometimes make such nodes to behave like malicious nodes in order to conserve their resources.
iii. Malicious nodes can collude to raise value and trust (in terms of rating) on one of the malicious nodes making it fit enough to raise alarms on good nodes as in CORE.
iv. Finally, there is no honest justice in the existing models of (IDS) algorithms as to how to prevent, detect and react accordingly to threats and intruders. Hence, an emergent need for improved intrusion detection system (IDS) algorithm.

1.9.4 My reasons for using 3-phase commit protocol

3-phase commit protocol has been used to successfully to prevent data inconsistency in the distributed database management system [8]. In the database context, a transaction is a sequence of database operation that must satisfy the following ACID properties [12];

A – Atomicity: Either all or none of the transaction operations are performed
C – Consistency: A transaction transforms the database from one consistent state to another consistent state. A database is said to be in a consistent state if all the data in the database satisfy a set of business rule.
I – Isolation: If several transactions are performed concurrently and the result of one transaction is isolated from the other.
D – Durability: A transaction is durable, if committed results are never lost.

In a distributed database management system, 3-phase commit protocol has been able to fix data consistency, despite the numerous clients on a global platform that perform transactions involving the same data.

Most malicious deeds often leave the data in the database in an inconsistent manner, violently violating the business rules enforced by the global database management system. It is strongly believed that being able to track intruders who attempt to introduce data inconsistency in the system would go a long way at sieving out malicious clients. Hence, my rational for using 3-phase commit protocol.

2 Conclusion

The newly improved intrusion detection system algorithm (IIDSA) serves to checkmate the weaknesses in the existing commonly known models of intrusion detection systems which are CONFIDANT, CORE, and OCEAN.

IIDSA integrates the functionalities of these three intrusion detection system algorithms and incorporate the concept of 3-phase commit protocol into its mode of operations in resolving threats. It is highly efficient in preventing, detecting, and reacting to threats and intrusion within the network especially in a mobile ad-hoc network.

The implementation of IIDSA is expected to be show-cased in the business process of R/3 systems. R/3 systems being a web-based application that exposes the organization to the threats inherited in mobile ad-hoc network need to sieve the business processes from being intruded.

The trend of communication by a way of voting introduced by IIDSA would make it an extremely difficult task for any potential hacker to succeed on any client or the global platform itself.

3 Recommendations

Meta-data in R/3 Systems are part of the systems that describe the data structure, processes (work-flows) as well as functions (modules) [11]. It is strongly recommended that all the modules that make up R/3 systems (*HR modules, Logistics modules, Material modules, Sales modules and so on)* which are partof the globally defined data in R/3 systems should exemplify IIDSA so that as the trends of transaction goes on hackers or malicious client would not be able to take advantage of the multi-user environment and perpetuate havoc.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Humayun Bakht. Centralized frame for routing in mobile ad-hoc network. Proceedings of ICCC; 2004.

[2] Rakesh Kumar Jha, Suresh V. Limkar, Upena D. Dalal. A performance comparison of routing protocol (DSR and TORA) for Security Issue in MANETs; 2010.

[3] Michiardi P, Molva R. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in Proceeding International Conference on IFIP Communications and Multimedia security (CMS'02). 2002;107–121.

[4] Bansal S, Baker M. Observation-based cooperation enforcement in Ad hoc Networks. Research Report cs.NI/0307012, Stanford University; 2003

[5] Buchegger S, Le Boudec J. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, Lausanne, Switzerland; 2002.

[6] Wayne Jansen, Tom Karygiannis. Mobile agent security NIST special publication. 1999;800-19.

[7] ITC System Education – Students Handout on Networking, "Wireless LAN Security". 2008;222-223. Available: www.itceducation.net

[8] James. Electronic notes in theoretical computer science. 2003;39(1):21-46.

[9] James Larson. Advanced database management systems. Three phase-Commit Protocol. 1995;142–144.

[10] Connolly Thomas, Begg Carolyn, Strachan Anne. Database systems, a practical approach to design, implementation and management. Addison-Wesley F; 1997.

[11] lorian Matthes, Stephen Ziemer. Understanding SAP R/3, a tutorial for computer scientists. The Integrated R/3 Repository. 1998;4. Available: http://www.sts.tu-harbug.de/f.matthes

[12] James Larson. Advanced database management systems. Distributed Transaction Processing. 1995;120.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
www.sciencedomain.org/review-history.php?iid=932&id=6&aid=7953