Fountain Journal of Natural and Applied Sciences: 2016; 5(2): 18-30

DOI: 10.53704/fujnas.v5i2.128

A publication of College of Natural and Applied Sciences, Fountain University, Osogbo, Nigeria.
Journal homepage: www.fountainjournals.com
ISSN: 2354-337X (Online), 2350-1863 (Print)

Modelling and Simulating Access Control in Wireless Ad-Hoc Networks

[1*]Azeez, N.A, [2]Otudor, A.E.

[1,2]Department of Computer Sciences, University of Lagos, Nigeria,

Abstract

There has been a great increase in the use of wireless networks over the years; Mobile Ad hoc Network is an example of such wireless network. It functions without any central administration and the network is made up of a collection of nodes within a radio frequency. Security in mobile network has been an area of great research over the years mainly because most ad hoc protocols do not provide the basic security framework and services. This paper aims at simulating access control in wireless ad-hoc networks. The objectives are to ensure that the network is not vulnerable and should also devoid of any form of malicious attack that could prevent authorized access. Two metrics (packet delivery ratio and traffic overhead) were used to measure the effectiveness and efficiency of the networks. Through a detailed simulation study, we show that the protocol is efficient and allows a trade-off between security and performance. This research focuses on designing an access control mechanism that was incorporated within ad-hoc routing protocols with the aim of adding an extra layer of security against threats in the network. The three stage-process for access control was implemented with NS-2 v 35. The nodes in the simulation were created dynamically, the movement between nodes was generated randomly and the connections between the nodes were done using Constant Bit Rate (CBR) connection which was aimed at enabling the network to mimic a real life scenario. Through different experiments and simulations done, it was observed that the access control model works and also provides a higher level of security for ad-hoc networks even when under security threats and attacks.

Keywords: Access control, NS 2, Ad-Hoc, MANET, Mobile, Simulation.

Introduction

The notion of "Access Control" is viewed among entities (e.g., domains, principals, components) engaged in various protocols as a set of relations established on the basis of a body of supporting assurance (trust) evidence and required by specified policies (e.g., by administrative procedures, business practice, law). In traditional networks, most trust evidence is generated via potentially lengthy assurance processes, distributed offline and assumed to be valid on long terms and certain at the time when trust relations

derived from it are exercised. Authentication and access-control trust relation established as a consequence of supporting trust evidence are later used in authorizing client relations and trust evidence are prevalent in mobile ad-hoc often

*Corresponding author: +2348035327365
Email address: nazeez@unilag.edu.ng

as certificates and as trust links (e.g., hierarchical or peer links) among the principals included in these relations or among their "home domains." Both certificates and access control are networks (MANETs) (Gorasia, Srikanth, Doshi and Rupareliya, 2016). Lack of a fixed networking infrastructure, high mobility of the nodes, limited-range and unreliability of wireless links are some of the characteristics of MANET environments that constrain the design of a trust establishment scheme.

In particular, trust relations may have to be established using only on-line-available evidence may be short-term and largely peer-to-peer, where the peers may not necessarily have a relevant "home domain" that can be placed into a recognizable trust hierarchy and may be uncertain. In this work, we argue that for access control in MANETs, a substantial body of trust evidence needs to be (1) generated, stored, and protected across network nodes, (2) routed dynamically where most needed, and (3) evaluated "on the fly" to substantiate dynamically formed trust relations. In particular, the management of trust evidence should allow alternate paths of trust relations to be formed and discovered using limited backtracking though the ad-hoc network, and should balance between the reinforcement of evidence that leads to "high certainty" trust paths and the ability to discover alternate paths. Although we focus on authentication and access-control trust in this work, similar notions can be defined for "correctness" trust relations required by system.

In an attempt to ensure that wireless ad-hoc network is not vulnerable and could also devoid of any form of malicious attack, the need to provide a dependable and reliable access control mechanism within the network is sacrosanct. If this could be achieved, information within the network will be properly secured and accessed by the authorised users.

Specifically in this work, we have been able to review different access control models such as Role Based Access Control (RBAC), Mandatory Access Control (MAC), Discretionary Access Control (DAC) and others. Efforts have finally been made to model and simulate access control in wireless ad-hoc networks with Network Simulator (NS-2) version 35 as the simulator. Packet delivery ratio and traffic overhead were used as metrics. With the results obtained, the access control framework in wireless ad-hoc network is efficient and effective.

Literature Review

A brief literature on Access Control and Ad-hoc Mobile Network shall be provided in this section. In the past few years, there have been discussions within the security community about the network security concept of protecting an information asset against unknown cyber-attacks. As a result, several hardware and software vendors have announced products that attempt to make this vision a reality. There are three popular security approaches used today (Nureni and Irwin, 2010). The following section exposes strengths and weaknesses of those approaches.

Traditional Access Control Models

There are two original access control models in information systems, which are Mandatory Access Control (MAC) and Discretionary Access Control (DAC) (Ferraiolo and Kuhn, 1992); Sandhu and Munawer, 1998). MAC manages access control levels by means of an administrator in the organization. It uses a hierarchical approach to control access to the objects, which represent system resources here. The administrator defines an access control policy that cannot be modified by the subjects. MAC is mostly used in the systems where priority is placed on confidentiality, such as in military applications. In a DAC model, the owner of an object controls access to that object. This means that he has power to create the permissions for data access. By default, subjects without this permission cannot access the objects. Subjects mean users here.

The concept of an access control matrix, which defines the relationships between subjects, objects and the actions that the subjects want to perform on the objects (Lampson, 1971). The subjects' identities are placed in rows and the objects' identities in columns. Each action that a subject wants to perform on an object is placed in the intersection of the corresponding row and column. The size of the access control matrix is directly proportional to the number of subjects and to the number of objects. Samarati and

Vimercati (2001) suggested that there are three possible approaches to implement the access control matrix in electronic systems, named authorization table, access control list (ACL) and capabilities. Among these, ACL and capabilities are commonly used in access control schemes.

The difference between ACLs and capabilities can be seen in Figure1.One of the drawbacks of using an access control matrix is that when there are a large number of subjects and objects in the system, the administration of those subjects and objects become very difficult to handle.

Access Control Models in Wireless Ad-Hoc

A considerable number of access control models has been proposed for use in AD-HOCs, though some of them are not yet implemented. In this section, we present the former access control models before we compare and contrast them in the next section. We group the proposed models into three main categories based on the nature of their architecture, namely: role-based access control (RBAC), cryptography-based access control (CBAC) and users' privacy preserving access control (UPPAC). Taxonomy of access control models for AD-HOCs, including the publication year of each proposal, is shown in Figure 2.

Role-Based Access Control (RBAC)

Most of the access control models in AD-HOCs and WMSNs are based on traditional RBAC which has been widely accepted as a policy-based access control model (Zhao and Chadwick, 2008). Applications based on RBAC have been implemented and deployed in commercial companies and education industries. The principle of RBAC model.

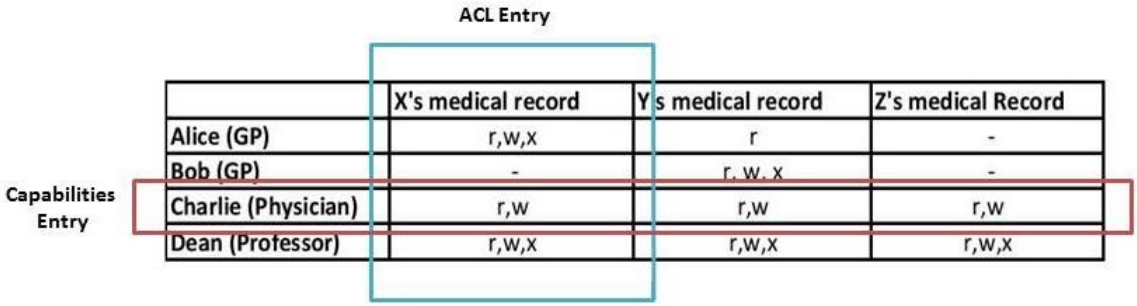

Figure1. Difference between access control list (ACL) and capabilities.

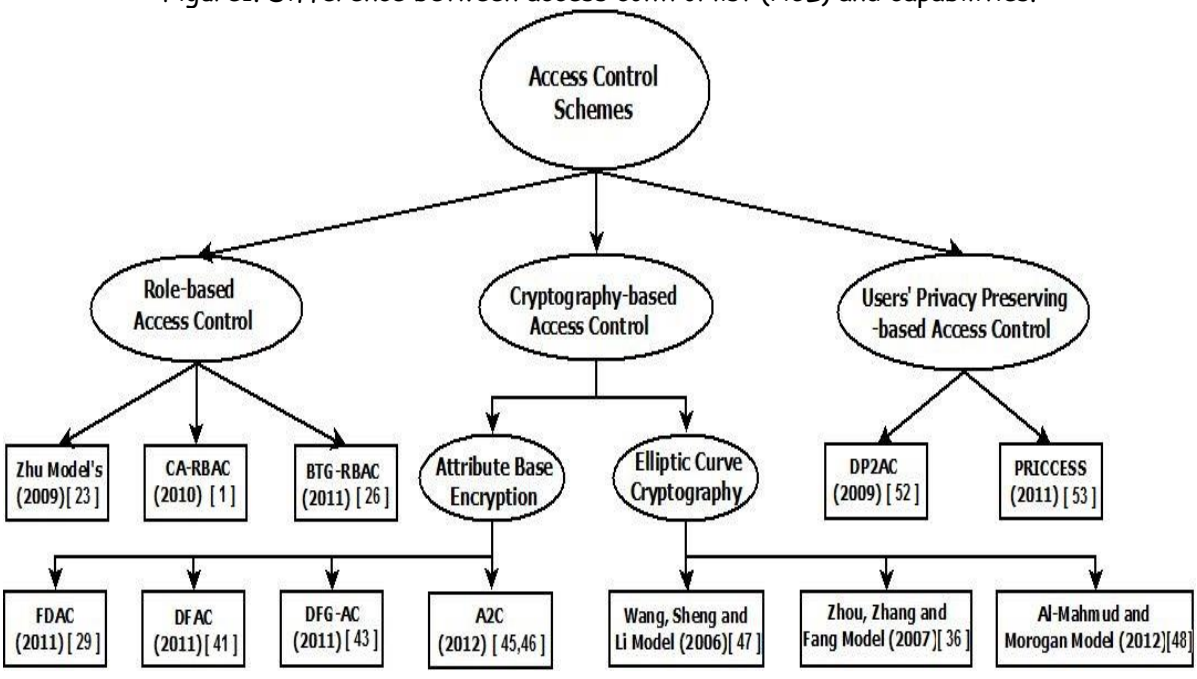

Figure 2.A taxonomy of access control schemes in AD-HOCs

is the role, defined as an intermediary concept relating a group of subjects to a set of access permissions. Any member from the subject group role has all of the permissions that are associated with that role. When a new subject is assigned to a group, he receives all of the associated access permissions, but these permissions are revoked when the subject leaves the group or is removed from the system. It is the same procedure to add and remove permissions from the roles. When a permission is added to a role, all of the members of the associated subject group will receive that permission. The permission will be revoked when it is deleted from the role. This feature helps to simplify system administration when there are many thousands of subjects and objects in an organization.

In RBAC, the access decision is a choice between two outcomes: permitted access or denied access. The following access control models are proposed based on the RBAC model with different extensions to provide further security properties in AD-HOCs. Figure 3 shows how RBAC-based access control models have evolved in the AD-HOC research community.

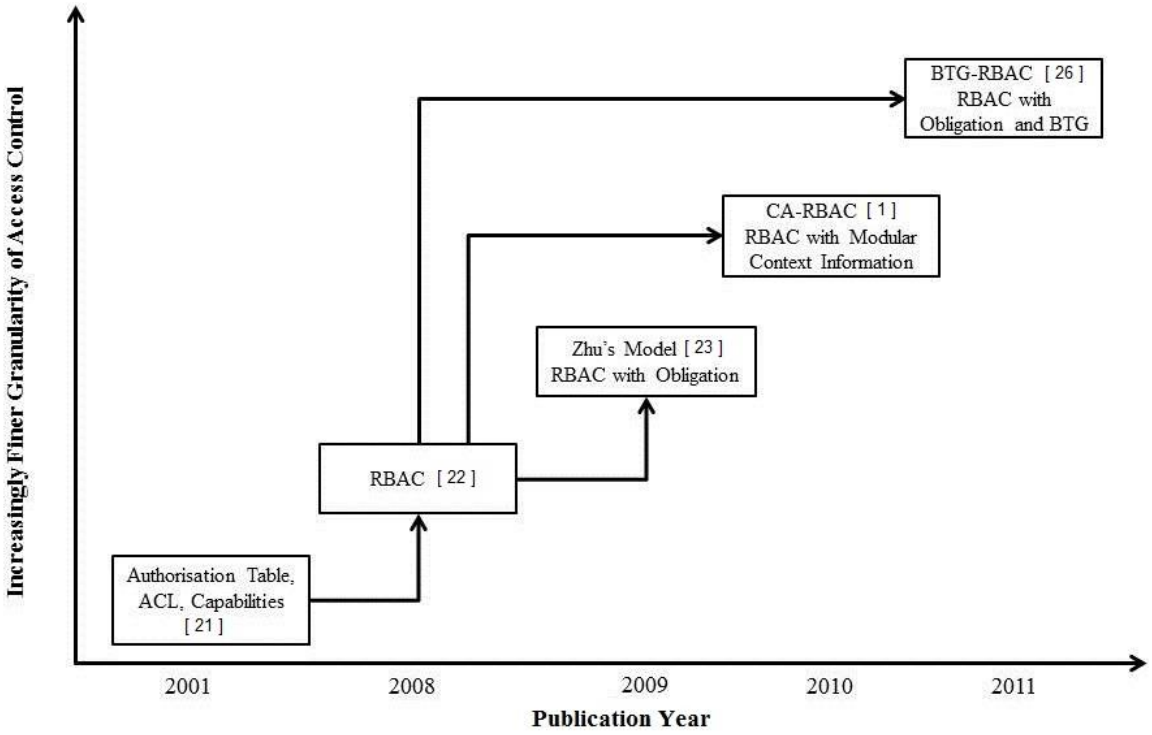

Figure 3. An evolution of role-based access control (RBAC)-based access control models in AD-HOCs.

Context-Aware Role-Based Access Control (CA-RBAC)

Garcia-Morchon and Wehrle (2010) proposed the context-aware role-based access control (CA-RBAC) model based on a modular context structure for WMSNs. The aim of the model is to provide context awareness and adapt its security properties to ensure the users' safety in WMSNs. Garcia-Morchon and Wehrle (2010) pointed out that the RBAC model is not good enough to use in an AD-HOC, because in traditional RBAC models, the roles and policies have to be predefined in advance. In the proposed model, the decision-making process is divided into three modular context situations: critical, emergency and normal condition. Based on these situations, the access privileges to sensed data will be different (Azeez and Babatope, 2016).

Break-the-Glass Role-Based Access Control (BTG-RBAC)

Ferreria et al (2011) proposed the break-the-glass role-based access control (BTG-RBAC) model based on the RBAC model. The main idea of this model is to gather necessary information from the end users with their collaboration for a usable

access control policy that can perform the BTG action in emergency situations. The break-the-glass (BTG) rule allows the users' to have emergency and urgent access to the system when a normal authentication does not perform or work properly. They introduced BTG rules in order to override access policy whilst providing non-repudiation mechanisms for its usage. In a real environment, unanticipated situations may occur because it is impossible to predict all of the access permissions in advance for all situations. The BTG extension is used for emergency and important cases whenever a user wants to access data urgently and immediately. The BTG-RBAC model made the system much more flexible than normal RBAC, but one of the disadvantages is that human processes are needed in order to enforce the BTG rules (Azeez and Ademolu, 2016).

Cryptography-Based Access Control (CBAC)

Cryptography-based access control (CBAC) is another form of access control model for the information systems. Ghani et al (2012) mentioned that the CBAC mechanism is designed for untrusted environments, where a lack of global knowledge and control are defining characteristics. It absolutely relies on cryptography to control data access and to ensure data confidentiality and integrity. The main idea is to use a unique key for each data resource. Users who are allowed to access that data resource are assigned the key for data access (Al-Hamdani, 2010). Cryptography methods in AD-HOCs should meet the constraints of sensor nodes, such as limited power, resources and memory shortage. Therefore, choosing a suitable cryptography method is important in AD-HOCs (Azeez and Venter, 2013).

Attribute-Based Encryption (ABE)-Based Fine-Grained Access Control

Goyal, Pandey, Sahai and Waters (2006) proposed the ABE scheme to model and design a scalable and flexible access control system. ABE is a public key cryptography primitive generalising identity-based encryption (IBE), which is associated with user's identity in a single user message (Gentry, 2006). In ABE, a group of users is described by the combination of several descriptive attributes and access structures, which is also called an attribute policy. In ABE, the public key encryption is based on one-to-many encryption. There are two different types of ABE, which are proposed by Goyal et al (2006), namely key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, data that is sensed and stored in the sensor node is encrypted with a set of attributes; the user's private key is associated with an access structure that specifies which types of ciphertexts the key can decrypt. Only the users that have the right access structure and the key can access and decrypt the sensed data. In CP-ABE, the ciphertext is associated with the access structure. The user's private key is associated with the attributes that specify which type of the ciphertext the key can decrypt (Azeez and Iliyas, 2016).

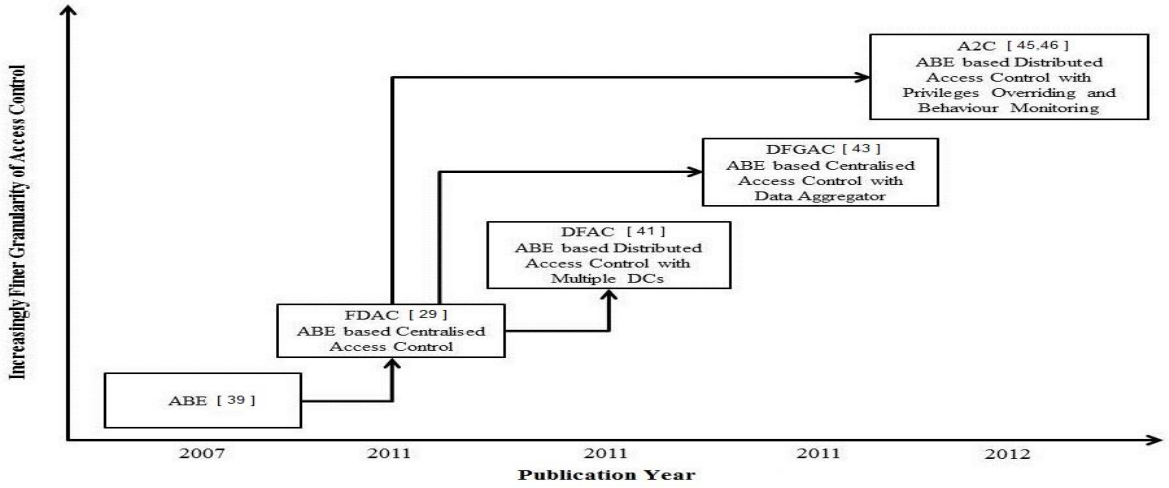

Figure 4: An evolution of attribute-based encryption (ABE)-based access control models in AD-HOCs (Fine-Grained Distributed Data Access Control (FDAC)). Source: Yu et al (2011)

Yu et al (2011) proposed the fine-grained distributed data access control (FDAC) model based on ABE. The main idea of their approach is to provide a distributed data access control, which is able to support fine-grained access control over sensor data and is resilient against attacks, such as user collusion (unauthorized users may collude to compromise the encrypted data) and node compromise (the sensor node could be compromised by a malicious user, due to lack of compromise-resistant hardware.). A network controller, which stores access structures, acts like a central distribution centre and distributes keys to users in FDAC. Only users with the right access structure and the right key can access data at the sensor nodes. The access structures will be different for each user depending on the access privileges of users.

Ruj et al (2011) proposed a fully distributed fine-grained access control (DFAC) scheme using multi-authority ABE Chase and Chow (2009) to prevent a single point of failure. Instead of using one authority, like FDAC, several distribution centres (DCs) are used to store and distribute different access structures, sets of attributes and cryptographic keys to users and sensor nodes. All DCs are disjoint from each other. Each DC has its own access subtree (a subtree contains attributes at the leaf nodes of that subtree.) for each sensor node. Users, who want to access data at the sensor node, need to activate their ID with each DC to obtain access structures, access subtrees and keys. All of the subtrees from each DC are ANDed together to build a complete access structure for a single user, but the user has to store all of the access structures in order to access different types of data from the sensor network. This model facilitates modification and secret key distribution when the access rights of a user are changed, but the communication overhead of the user's revocation process is higher than with FDAC.

Hur (2011) proposed an access control model called distributed fine-grained data access control (DFG-AC). It uses both a network controller and a data aggregator for central key management and central storage. The collected data from sensor nodes are transferred to the data aggregator by using a distributed sensor data collection protocol, such as the Two-Tier Data Dissemination protocol (TTDD) (Ye et al., 2002). The main idea of using the data aggregator as central storage is to perform more data encryption. Additionally, the users can get all of the information by accessing the data aggregator. The data aggregator is more powerful than the sensor nodes, and it can use complex encryption methods. The advantage of the proposed model is that it considers the stateless receiver problem. (Practically, users may miss a key update message. Therefore, they cannot keep their key states up-to-date. This problem is known as the stateless receiver problem.) To solve this problem, key revocation is done with a stateless group key distribution mechanism using a binary tree. One of the disadvantages is that the transmitting data from sensor nodes to the data aggregator consumes lots of battery power and energy. In addition, there might be a single point of failure because of the centralised data storage. This model provides user revocation by using the KP-ABE scheme with the attributes for distributed AD-HOCs (Azeez and Lasisi, 2016).

Wang et al (2006) proposed an access control model based on ECC. The main objective of the proposed model is to use an ECC scheme for granting user access rights to the collected data. Different users may have different levels of data access due to restriction of access implicated by the data confidentiality and privacy. ECC is used in key distribution and sharing information between the users and a key distribution centre (KDC). In this approach, KDC is responsible for generating all security primitives, such as random numbers, access lists and hash functions, and maintains a user list with associated user identifications (Azeez and Venter, 2013). The users have to request access permission from KDC. Access lists, which comprise user identity, group identity and user privilege mask, define the user's access privileges. User access privilege mask is a number of binary bits, and each bit represents a specific information or service. Therefore, users who possess the same mask and access privileges are put in the same group (Azeez, Iyamu and Venter, 2011).

Al-Mahmud and Morogan (2012) proposed an identity-based authentication and access control model in AD-HOCs. The main idea of the proposed model is to use an identity-based signature (IBS) for providing both user

authentication and data access control in AD-HOCs (Shamir, 1985). This protocol is based on the IBS scheme, where an ECC-based digital signature algorithm (DSA) (Johnson, et al., 2001) is used to sign and verify a message. A base station (BS) is responsible for generating the private keys of both users and sensor nodes in the network. For the key distribution, a one pass key establishment protocol Wang et al (2011) is used to share session keys between sensor nodes and users. Users are required to register with BS. Based on the access request from the users, BS generates private key and access structure for each user. The sensor nodes are preloaded with hash value of user identities and the private key, which will be used for the authentication process. After the authentication process, the sensor node will check whether the user is authorized to access the data (Al-mahmud and Morogan, 2012).

Access Control Procedural Phases

The access control mechanism will be initiated in three basic steps.

Step 1: The network nodes are set-up to form a node to node cache in the network layer, the cache will work as a watchdog which will notify all node in the network for any irregular behaviour to gain network resource access.

Access Control Phase 1

```
# Creating underlying cache
for {set i 0} {$i< $value(nnaodv)} {incri} {
set node_($i) [$ns_ node]
    $node_($i) random-motion 0 ;#disable random motion
    }
for {set i $value(nnaodv)} {$i< $value(nn)} {incri} {
set node_($i) [$ns_ node]
    $node_($i) random-motion 0 ;#disable random motion
    [$node_($i) set ragent_] malicious
    $node_($i) label " Node"; #Labeling the node
}
# Connection Parameters
# from /indep-utils/cmu-scen-gen/setdest..
# ./setdest -n 20 -p 1.0 -M 20.0 -t 500 -x 750 -y 750 > test
set god_ [God instance]
source $value(cp)
# CBR Connections generated by cbrgen.
```

It is done from ns-2.35/indep-utils/cmu-scen-gen using the command below.

Step 2: This step is to verify any malicious activity against the threshold defined to see if there a match. See connections:

Access Control Phase 2

```
for {set i 0} {$i< $connections } {incri} {
    $ns_ at $value(cstop) "$cbr_($i) stop"
    }
# Tell all nodes when there is a match
for {set i 0} {$i< $value(nn) } {incri} {
    $ns_ at $value(stop) "$node_($i) reset";
```

Step 3: This step will be to flush out or block the malicious node from using any network resource

Access Control Phase 3

```
proc finish {} {
global ns_ trace_bnam_trace
    $ns_ flush-trace
close $trace_b
close $nam_trace
proclabeling {nid1 nid2 cbrid} {
        global node_
        $node_($nid1) label "Sending cbr_($cbrid)"
        $node_($nid2) label "Receiving cbr_($cbrid)"
}
End.
```

Design and Implementation

The simulations were carried out using NS2, as it enabled us to test different network scenarios. The nodes in the simulation were created dynamically, the movement between nodes was generated randomly and the connections between the nodes was done using Constant Bit Rate (CBR) connection, this was to enable the network mimic a real life scenario as close as possible. The connection type used was UDP and not TCP; this is because UDP packets would enable to measure the packets loss in the network properly. Adopting using TCP would have made this almost impossible as TCP would assume packets dropped were lost in the network and would keep sending

more packets until it receives an acknowledgement packet form the receiving node.

Figure 5 shows the metric for the simulation. It shows the number of nodes, the simulation area, simulation length and the output files.

Figure 6 shows how nodes in the network are configured in the TCL script. The properties of the node are firstly set, line 52 to line 55 shows the dynamic creation nodes. Different simulation metrics were during the course of this research, the different simulation scenarios are listed below.
20 AODV nodes
AODV, DSR and the access control mechanism.

Table 1 - Simulation traffic parameters

Simulator	NS2
Area	800 X 800
Simulation time	60 SEC
Traffic type	UDP
Data payload	512 BYTES

Table 2- Simulation scenario parameters

Routing protocol	AODV, DSR
Number of nodes	20
Number of mobile nodes	20

```
1  set value(chan)          Channel/WirelessChannel                ;#Channel Type
2  set value(prop)          Propagation/TwoRayGround                ;# radio-propagation model
3  set value(netif)         Phy/WirelessPhy                         ;# network interface type
4  set value(mac)           Mac/802_11                              ;# MAC type
5  set value(ifq)           Queue/DropTail/PriQueue                 ;# interface queue type
6  set value(ll)            LL                                      ;# link layer type
7  set value(ant)           Antenna/OmniAntenna                     ;# antenna model
8  set value(ifqlen)        150                                     ;# max packet in ifq
9  set value(nn)            20                                      ;# total number of mobilenodes
10 set value(nnaodv)        19                                      ;# number of AODV mobilenodes =
11 set value(rp)            AODV                                    ;# routing protocol
12 set value(x)             750                                     ;# X dimension of topography
13 set value(y)             750                                     ;# Y dimension of topography
14 set value(cstop)         50                                     ;# time of connections end
15 set value(stop)          60                                     ;# time of simulation end
16 set value(cp)            "testAODV"          ;#Connection Pattern
17 set value(cc)            "cbrgenerate"                          ;#CBR Connections
18 # Initialize Global Variables
19 set ns_ [new Simulator]
20 $ns_ use-newtrace
21 set trace_b [open blackhole.tr w]
22 $ns_ trace-all $trace_b
23 set nam_trace [open blackhole.nam w]
24 $ns_ namtrace-all-wireless $nam_trace $value(x) $value(y)
25
```

Figure 5 - Wireless topology configurations

```
36 # configure node, please note the change below.
37 $ns_ node-config          -adhocRouting $value(rp) \
38                           -llType $value(ll) \
39                           -macType $value(mac) \
40                           -ifqType $value(ifq) \
41                           -ifqLen $value(ifqlen) \
42                           -antType $value(ant) \
43                           -propType $value(prop) \
44                           -phyType $value(netif) \
45                           -topoInstance $topology \
46                           -agentTrace ON \
47                           -routerTrace ON \
48                           -macTrace ON \
49                           -movementTrace ON \
50                           -channel $chan_1_
51
52 # Creating mobile AODV nodes for simulation
53 for {set i 0} {$i < $value(nnaodv)} {incr i} {
54         set node_($i) [$ns_ node]
55         $node_($i) random-motion 0     ;#disable random motion
56         }
57
58 # Creating Black Hole nodes for simulation
59 for {set i $value(nnaodv)} {$i < $value(nn)} {incr i} {
60         set node_($i) [$ns_ node]
61         $node_($i) random-motion 0     ;#disable random motion
62         [$node_($i) set ragent_] malicious
63         $node_($i) label "Blackhole Node"; #Labeling the node
64 }
```

Figure 6: Node configuration

Results and Discussions

Two metrics were used to measure the effectiveness of the network and the entire simulation carried out. The metrics are: packet delivery ratio which measures the percentage of packages sent and what is received and also the traffic overhead which is a measure of how much data is in the network.

Table 3 and 4 show the statistical representation of the simulation values in percentages of the different simulations done. The values are later plotted into a graph to give a visual representation of how the different simulation metrics were combined together.

Figure 7 is a simulation snapshot of the access control experiment. The two red nodes are trying to gain access to restricted network resource and have been flagged in the networks, packet generated or sent by these nodes will not be routed by other nodes in the network

Table 3: Traffic Overhead

TRAFFIC OVERHEAD /SEC	ACCESS CONTROL (%)	AODV (%)	DSR (%)
10	80	45	43
20	60	43	40
30	45	35	38
40	42	30	32
50	41	28	34

Table 4: Packet Delivery Ratio

PACKET DELIVERY RATIO (%)	ACCESS CONTROL (%)	AODV (%)	DSR (%)
20	36	60	47
40	41	69	59
60	54	72	70
80	69	84	84
100	78	95	93

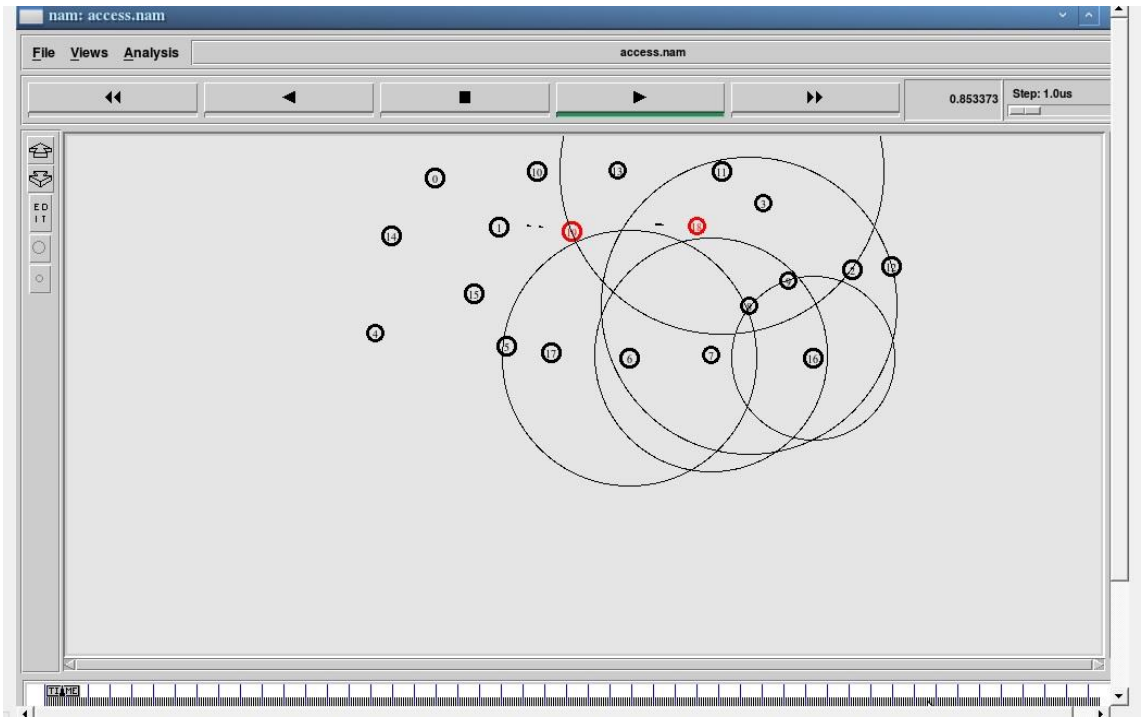

Figure 7: Simulation Snapshot

.

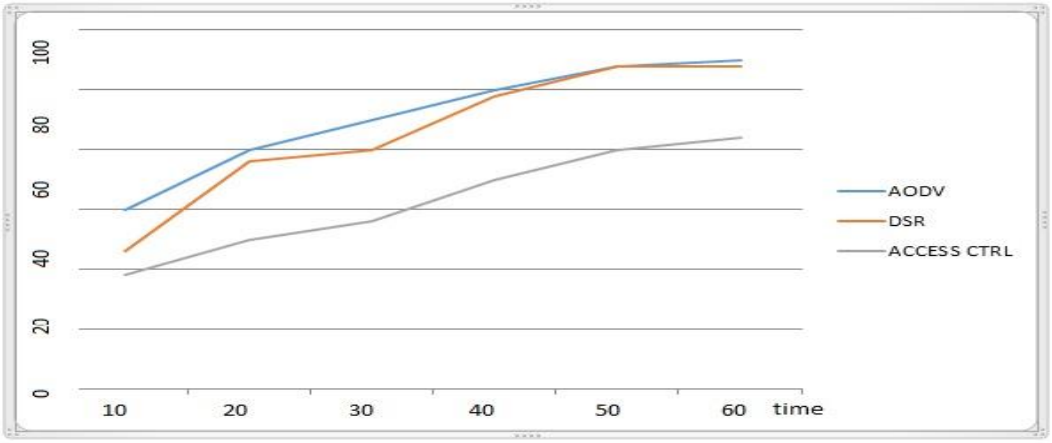

Figure 8: Package delivery ratio

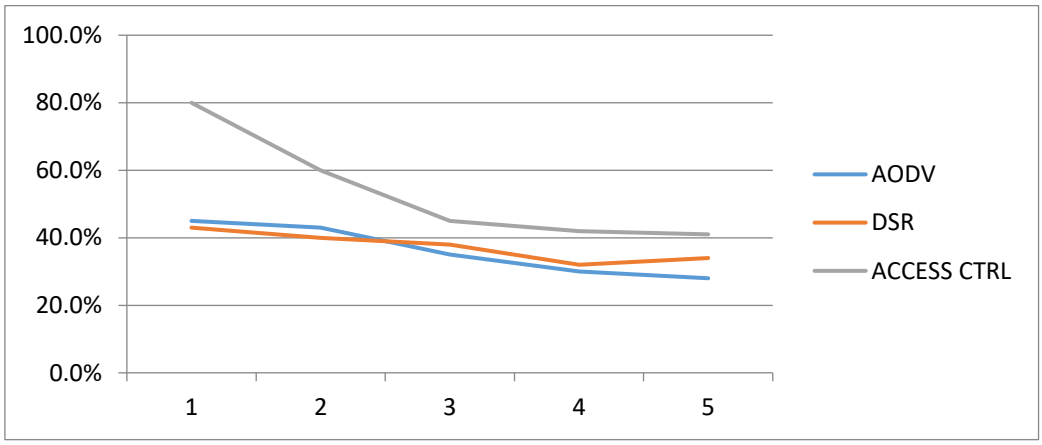

Figure 9 – Traffic Overhead

Figure 8 shows that traffic delivery ratio increases slightly with the access control mechanism (node velocity is set constant). This is mainly due to the trust termination process, whereby a node temporarily terminates its trust on another node if it has not heard from that node for a time interval. Two cases may cause two nodes to temporarily lose contact in one time interval but regain contact later on. The first case is when a HELLO message is lost; the second case is when a node moves out of the transmission range of the other but moves in again quickly. In the simulation, a node drops packets from another node when their old trust has been terminated while their new trust has not been established yet. It is noted that the larger the time interval, the less likely that two nodes completely lose their contact in the interval, thus the larger the packet delivery ratio. It is noted that packet delivery ratio could be further improved if a node temporarily buffers the unverifiable packets until their trust (re)establishment process is completed.

Figure 9 shows that traffic overhead decreases with the access control mechanism, this is because more data is sent among the nodes in terms of node authentication thus the reason for the extra overhead Secondly, the traffic overhead grows at a lower rate as node velocity increases, because the chance that a node meets new nodes does not increase linearly with its velocity due to the limited size of a network. The figure also shows the traffic overhead is larger than in AODV and DSR. This is due to different traffic patterns used in the simulations.

Summary and Conclusion

The designed access network protocol is a lightweight hop-by-hop authentication protocol for network access control in ad hoc networks. It is based on two techniques: (i) hop-by-hop authentication for packet authentication and for reducing the overhead for establishing trust among nodes. The design of the access control system is transparent and independent of the routing

protocols. Through a detailed simulation study, we show that the protocol is efficient and allows a tradeoff between security and performance. It can be seen that the access control systems upgrades overall network performance in a malicious environment, though certain network metrics are affected but overall throughput is improved. After multiple simulations to understand the effects of lack of access control mechanism, it is imperative that an adhoc network protocol suffers from security attacks. During the simulations, effort was made to monitor the performance metrics of each like delay, packet loss, throughput and routing overhead in each simulation carried out. After analysing the output files from each simulation, it can be seen that the mechanism truly performs well.

Future Work

The developed access control system can improve on in future to reduce the malicious effects of more security attacks. It can also be improved to work with more ad hoc routing protocol and not just AODV and DSR, it can further be developed to work with table driven protocols.

References

Al-Hamdani, W. (2010, October 1 - 3). Cryptography based access control in healthcare web systems. *2010 Information Security Curriculum Development Conference (InfoSecCD '10)* , 66 -79.

Al-mahmud, A., & Morogan, M. (2012). Identity-based authentication and access control in wireless sensor networks. *Int. J. Comput. Appl.* , 41, 18 - 24.

Azeez, N. A., & Ademolu, O. (2016). CyberProtector: Identifying Compromised URLs in Electronic Mails with Bayesian Classification. *2016 International Conference Computational Science and Computational Intelligence (CSCI)* (pp. 959-965). Las Vegas, NV, USA: IEEE.

Azeez, N. A., & Babatope, A. B. (2016). AANtID: an alternative approach to network intrusion detection. *The Journal of Computer Science and its Applications. An International Journal of the Nigeria Computer Society* , 129-143.

Azeez, N. A., & Iliyas, H. D. (2016). Implementation of a 4-tier cloud-based architecture for collaborative health care delivery. *Nigerian Journal of Technological Development , 13* (1), 17-25.

Azeez, N. A., & Venter, I. M. (2013). Towards ensuring scalability, interoperability and efficient access control in a multi-domain grid-based environment. *SAIEE Africa Research Journal , 104* (2), 54-68.

Azeez, N. A., Iyamu, T., & Venter, I. M. (2011). Grid security loopholes with proposed countermeasures. In E. Gelenbe, R. Lent, & G. Sakellari (Ed.), *26th International Symposium on Computer and Information Sciences* (pp. 411-418). London: Springer.

Azeez, N.A., & Lasisi, A. A. (2016). Empirical and Statistical Evaluation of the Effectiveness of Four Lossless Data Compression Algorithms. *Nigerian Journal of Technological Development, Vol. 13, NO. 2, December 2016, 64-73.*

Bender, A., Katz, J., & Morselli, R. (2008). *Ring signatures: Stronger definitions, and constructions without random oracles.* J. Cryptol.

Chase, M., & Chow, S. (2009, November 9 – 13). Improving privacy and security in multi-authority attribute-based encryption. *16th ACM Conference on Computer and Communications Security* .

Ferraiolo, D., & Kuhn, D. (1992, October 13 - 16). Role-based access controls. *15th National Computer Security Conference* .

Ferreria, A., Correia, R., Monterio, H., Brito, M., & Antunes, L. (2011, June 27 - 30). Usable access control policy and model for healthcare. *2011 24th International Symposium on Computer-Based Medical Systems (CBMS)* , 1 - 6.

Garcia-Morchon, O., & Wehrle, K. (2010, June 9 - 11). Modular context-aware access control for medical sensor networks. *15th ACM Symposium on Access Control Models and Technologies (SACMAT '10)* , 129 - 138.

Gentry, C. (2006). *Handbook of information Security.* John Wiley and Sons: Bakersfield, CA, USA.

Ghani, N., Selamat, H., & Sidek, Z. (2012). Analysis of existing privacy-aware access control for e-commerce application. 12, 1- 5.

Gorasia, N., Srikanth, R., Doshi, N., & Rupareliya, J. (2016). Improving Security in Multi Authority Attribute Based Encryption with Fast Decryption. In K. Mishra (Ed.), *Proceedings of International Conference on Communication, Computing and Virtualization (ICCCV) 2016* (pp. Proceedings of International Conference on Communication, Computing and Virtualization (ICCCV) 2016). Elsevier.

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM conference on computer and communications security (pp. 89-98). Alexandria, Virginia, USA.

He, D., Bu, J., Zhu, S., Chen, C., & Chan, S. (2011). *Distributed access control with privacy support in wireless sensor networks.* IEEE Trans. Wirel. Commun.

Hur, J. (2011). *Fine-grained data access control for distributed sensor networks.* Wireless. Network.

Lampson, B. (1971, January). Protection. *5th Princeton Conference on Information Sciences and Systems* .

Morchon, O., & Wehrle, K. (2010, 29 March - 2 April). Efficient and context-aware access control for pervasive medical sensor networks. *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)* .

Nureni , A. A., & Irwin, B. (2010). Cyber security: Challenges and the way forward. *Computer Science & Telecommunications, 29*, 56-69.

Ruj, S., Nayak, A., & Stojmenovic, I. (2011, May 16 - 20). Distributed fine-grained access control in wireless sensor networks. *2011 IEEE International Parallel and Distributed Processing Symposium (IPDPS)* , 352 - 362.

Samarati, P., & Vimercati, S. (2001). Access control: Policies, models and mechanisms. *Foundation of Security Analysis and Design , 2171*, 137 - 196.

Sandhu, R., & Munawer, Q. (1998, October 22 - 23). How to do discretionary access control using roles. *3rd ACM Workshop on Role-Based Access Control* .

Sen, J. (2009). A survey on wireless sensor network security. *International Journal of Communication Network Information Security* , 1, 55 - 78.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes. *Advances in Cryptology , 196*, 47 - 53.

Wang, H., Sheng, B., & Li, Q. (2006). Elliptic curve cryptography based access control in sensor networks. *Int. J. Secur. Netw.* , 1, 127 - 137.

Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. *IEEE Community Survey* , 8, 20 - 23.

Wang, Y., Wong, D., & Huang, L. (2011, June 5 - 9). A one-pass key establishment protocol for anonymous wireless roaming with PFS. *2011 IEEE International Conference on Communications (ICC)* , 1 - 5.

Ye, F., Luo, H., Cheng, J., Lu, S., & Zhang, L. (2002, September 23 – 28). A two-tier data dissemination model for large-scale wireless sensor networks. *8th Annual International Conference on Mobile Computing and Networking (MobiCom'02)* , 148 – 159.

Yu, S., Ren, k., & Lou, K. (2011). Fdac: Toward fine-grained distribution data access control in wireless sensor networks. *IEEE Trans. Parallel Distribution System* , 22, 673 - 686.

Zhao, G., & Chadwick, D. (2008, June 23 - 25). On the modeling of bell-lapadula security policies using RBAC. *2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE '08)* , 257 - 262.

Zhou, Y., Zhang, Y., & Fang, Y. (2007). *Access control in wireless sensor networks.* Ad Hoc Network.

Zhu, Y., Keoh, S., Sloman, M., & Lupu, E. (2009). A lightweight policy system for body sensor network. *IEEE Trans. Netw. Serv. Manag* , 6, 137 - 148.

Zhu, Y., Keoh, S., Sloman, M., Lupu, E., Zhang, Y., Dulay, N., et al. (2008, 29 September - 2 October). Finger: An effective policy system for body sensor networks. *5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems* , 428 - 433.