Efficient Dynamic Streaming By Resolving Firewall Anomalies in Mobile AdHoc Networks

Prasanthi potnuru[1] Tatapudi.prabhakara Rao[2]
[1](Final Year M.Tech ,Dept. of CSE,Aditya Institute of Technology and Management(AITAM), Tekkali,Srikakulam,Andhra Pradesh ,prasanthi35@gmail.com)
[2](Asst.Professor, Dept. of CSE,Aditya Institute of Technology and Management(AITAM), Tekkali,Srikakulam,Andhra Pradesh,prabhakar.tatapudi@gmail.com)

Abstract:

The Computational technology of various service oriented systems and clouds are enable us to do processing. The sufficient and efficient performance results were generated by this service oriented systems. Though, we also suffered from various insecurity attacks while transmitting data or in system communication. But in previous many secure providing algorithms are proposed. Among them firewalls are conditional rules for protecting communication between systems. Always the migration of the new firewall adoptions for current network protocols is challenging task. Some networks cannot migrate to firewalls from legacy structure to new or innovative firewall (properties/polices). This could be based various reasons of old or legacy with some range of protocols, cross environment migration for communication issues in firewall enabled infrastructure. So to overcome these issues first we take nodes in MANET (mobile AdHoc network) structure for casting communications. Always casting communications are trust worthy for transmissions. In this MANET we adopt only single casting infrastructure to put dynamic firewalls in various parameters.

Key Terms:

(Firewall, MANET, Anomalies, Aggregation, casting, Access control)

1. Introduction

The essential element which was mainly used in networks and information system security, that is Firewall, are widely implemented. The firewall is protecting the system by communicating the outside people to change configurations of current system. Firewalls have been broadly deployed in protecting mistrustful traffic and unofficial right to use to net services enterprises. Sitting on the border between a private network and the global internet, a firewall examines all incoming and outgoing packets based on security rules. To implement a major security policy in a firewall, system administrators define a set of scrutiny rules that are derived from the organizational network security requirements.

Firewall policy management is a challenging task due to the complexity and Interdependency of policy rules. This is further exacerbated by the continuous evolution of network and system environments. Firewall policies have security flaws. The process of configuring a firewall is tedious and complicated for transmission. Therefore, effective mechanisms and tools for policy management are crucial to the success of firewalls.

Recently, policy anomaly detection has received a great deal of attention Corresponding policy analysis tools. Here in this paper we generate policy anomaly preventions in MANET (mobile adhoc networks.). Manet is a wireless communicated network. Once the network is established, the routes are monitored continuously by aggregated flows. In This Approach we proposed new framework on MANET (Mobile Ad Hoc Network).here in Manet Network the flows are distributed as Single Cast, Multicast, Broadcast. The Distributed Control plan is applied to each secure multipath aggregation

through the Manet. Centralized forwarding from Root node to all nodes which was in Manet will be secured by the connectivity. The Experiment results evolves the simulation results are included to validate the performance of this framework.

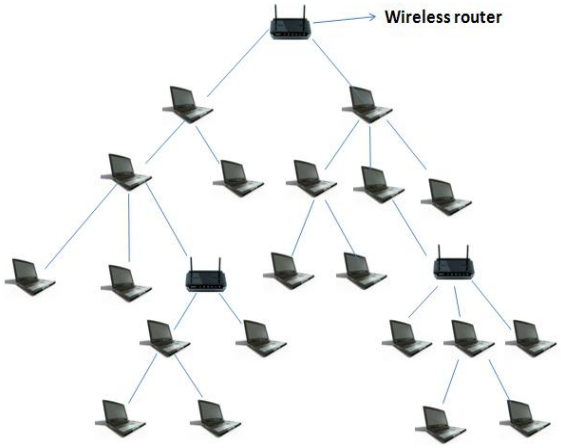
The mobile AD Hoc Network framing is created. The many nodes have to be generated by levels. Here the flow will be go though the Manet in 3ways.Those are Single cast, Multi Cast, Broad Cast. In Single cast, the flow will be done through from one node to particular nodes. In Multicast the Flow will be done through multiple nodes to certain nodes. In Broad Cast, The Flow will be done through Root Node to any node in Manet.

due to the complex nature of policy anomalies in Existing system we introduce new approach which id firewall implementation implemented in MANET. Because the wireless communication is completely unsecure rather than wired networks. Because of broadcasting. This is a challenging task to resolve the problem when occurring anomalies and conflicts in wireless.

2.Network Model:

Create a Wireless network which is known as MANET that is having number of level nodes. Each level should have one router for monitoring those respective level nodes. The MANET contains Main router as a Root for all these Level nodes of wireless network. The routers in each level are also called as trusted nodes. These trusted nodes will become act as secure nodes to permit the transactions between different levels of nodes. the Root Trusted node manage the all levels of trusted nodes information within their logs for finding the Firewall anomalies such as Data Leakage, data damage, missing order of data. In transmission we are using TCP and UDP Protocol.

Hierarchical tree MANET



Network framing:

Algorithm

Notation:

$\sum_{o}^{n-1} M$ ← *Manet tree with N nodes*

$\sum_{0}^{n} S$ ← *Segmentation vector*

$P_{P\_}$ ← *Policy set where P is the set of all available policies*

L ← *level of the manet*

n_l ← *node at level*

RESTR (M, n_l*)* ← *(a, d, m) // function to restructure the available manet*

R_l ← *rule for level*

Level weightage with HOPS

Level	Available Nodes	Total nodes
0	1	1
1	2	3
2	4	7
3	8	15

Traversing through the network algorithm:

Initialization

Step 1: M ← o

n ← 0

l ← 0

k ← 0

step 2: n ← dynamic input

loop for each k in n

if $2^k \leq n$

l ← k

end loop;

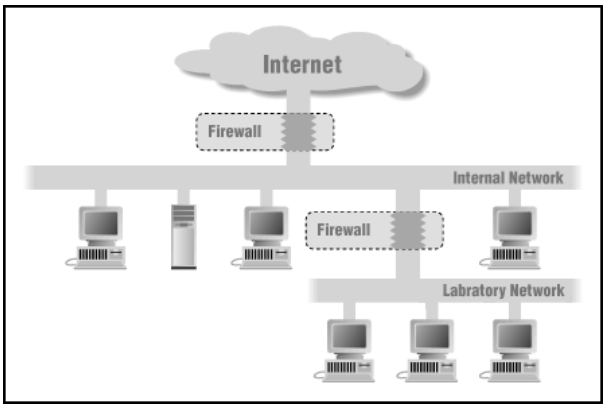
step 3: Accom (M, l, n)

M ← $\sum_0^{n-1} node(n_l)$

Firewall Policies:

Basically we put three firewalls (unique policies) to migrate from one firewall to another without cost / time/ infrastructure issues. So these policies are based on firewall migration but with dynamic and reducing the migration speed with the current migration speed without changing the dedicated casting paths, but modifications if not trust worthy or not satisfying threshold manet.

All the rules/policies for each firewall will be generated by the algorithm MRMPF(manet rule migration per firewall). Which is having 3types of firewalls and each firewall is having policies for faster migration from one to another without changing the regular scenarios.



Firewall Architecture

Default Firewall

Basically whenever the MANET is generated by MANET algorithm with the dynamic node (number of nodes), this firewall is attached to MANET. The property/policy of this firewall is to find no of dedicated trust paths by putting the threshold aggregate % of communications (ex 65%).If the path is not up to mark i.e. always less than threshold percentage the path will be blocked and the path will be in directed by the other main paths. So the regular casting will be in directed but transmitted without any issues.

Hops Structuring:

$N_1 \rightarrow$ {n3,n5,n7} =n2={n1,n4,n5}

Policy1:

Input: ∑s(n) ←source node vector

Input: ∑d(n) ←destination node vector

Output :$\sum_0^n N$

Loop: for each s_d in n ←source destination combination

start

$\sum t_s \leftarrow s$

$\sum t_d \leftarrow d$

temp←combination ($t_{s,,}t_d$)

T<=∑s(n)→∑d(n)

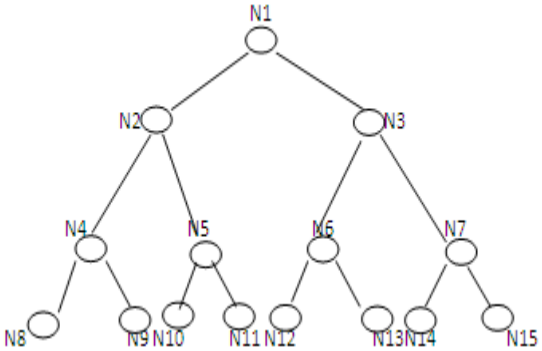
End loop

N=∑s(n)u∑d(n)

In this algorithm first we take source node and destination nodes are input and we are getting output is total number of count that means how many nodes are participating in the communication. For this first take a loop for finding source and destination combination .total no of source nodes are assigned to ts vector. Total no of destination nodes are assigned to td vector. Each level source and destination nodes combination is assigned to temp variable. Then check the threshold value if it is greater than 65% then it is proper communication. Then add the count i.e total number nodes to n variable. If the threshold value if it is less than 65% then it is not proper communication and it is considered as an anomaly. Then it is blocked.

Firewall artificial1

All the levels in the Manet will be having one dedicated router and this router is dedicatedly used to transmit packets indirectly. Once if source accidentally migrated to router then the router will change the source in the available nodes in that level (but by finding trustworthy node based on frequency of communication). For example we are taking the nodes n1, n2, n3….,n10 are in the manet. in these nodes n3,n5,n7are the trusted routers nodes.n3wants to send the packets to n6,n8,n10 this is done properly.now n4 node wants to send packets to n6,n8,n10 but this is not the trusted node then it send request to rootnode,n3 for getting the permission. Then both nodes are giving the permission to n4 for sending data to n6, n8…, n10. Then n4 node is sending the packets to those nodes properly.



Policy2 (firewall artificial 1):

Input: levels (no of levels in manet)

Output: router tracing

For each l in total no of levels

Loop start:

Temp R← find router (l)

For each node in s(source node)

If node==temp R

r ←reassign(l_n)

∑R← r //R is router vector in all levels

End loop

In this algorithm we are take router in each level as input and we are getting output is tracing the routers. For all levels find the routers and assigned to tempR variable. If source node is equal to router node then reassign the sourcenode.thne and the loop.

Firewall artificial2

Basically the communication of the packets is only through "routers". If a (n1) is the source node and n6 is the destination node always these packets will be transmitted to router first and the router will be routing the packets to the destination. In this scenario if the communication is in any duplication with the other regular communications, this communication will become subset and the super set will become the regular transmission path for this path. This reduces redundancy.

Policy3 (firewall artificial2):

Input →R //routers in all levels

Output →∑path

For each l in total no of levels

Loop start:

Assume n_l is source

Assume d_l.....d_{l-n} are destinations

If(n_l € R)

Continue;

Else

path←dup($n_l \rightarrow d_{l-n}$)

l++;

end loop;

In this algorithm we take the input as routers in all levels, and we are getting out put as find the shortest path. For this check all levels contain source nodes those are assigned to **nl** and destination nodes are assigned to **dl**. If **nl** is belongs to R then continue the process. And add the path to upland finally get the shortest path.

Rule Applicable on MANET:

Assumed policies in the network are ***{p1,p2,p3,p4,p5}***

Manet rule migration per firewall:

in manet network framing each level of trusted nodes fallow the firewall policies like below. The root trusted node doesn't follow any policies it just managing the all trusted nodes which are in all levels of wireless AdHoc network. Here at level 1, Policy p1 having 2 rules r1and r2. At level 2, policy p2 having 3 rules r3, r1, r4. Up to p5 of level 5 .

Segmented policies:

Level	Segment	Policy
0	0	-
1	1	$P_1(r_1,r_2)$
2	1	$P_2(r_3,r_1,r_4)$
3	2	$P_3(r_4,r_6,r_1)$
4	2	$P_4(r_2,r_4,r_1,r_5)$
5	3	$P_5(r_5,r_4,r_2,r_1)$

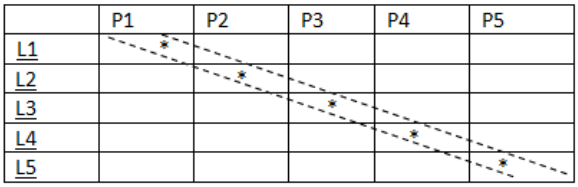
Each policy follows corresponding rules as below given.

Rules indicator/policy

	R1	R2	R3	R4	R5
P1	*	*			
P2	*		*	*	
P3	*			*	
P4		*		*	*
P5	*	*		*	*

Each level of MANET applicable with each different policies like below.

Policy duplicator reduction/level



Finding Anomalies:

Basic communications for TCP and UDP:

Normally for transmission in networking we need to follow above 2 protocols. To use these protocols 2 attributes/parameters are required(Ip, port).

Rules existing

Table:

Rule1	TCP Ip1 | Ip2 × √	UDP Ip1 | ip2 √ ×	Port 120 TCP(120) √ × / UDP(120) × √
Rule2	Ip1 |ip2 ×	Ip1|ip2 √	Port 202 TCP(202) × / UDP(202) √
Rule3	Ip1 | ip2 √	Ip1 |ip2 √	Port306 TCP(306) √ | / UDP(306) | √
Rule4	Ip1 | ip2 ×	Ip1 | ip2 ×	Port401 TCP(401) ON √ / UDP(401) ON √
Rule5	Ip1 | ip2 √	Ip1 | ip2 √	Port405 TCP(405) √ON × × ON √ / UDP(405) × ON √ √ ON ×

Estimated IPs: source- 203.678.54.3

Destination – 203.678.54.8

Rule1: source and destination is under two communications tcp and udp. If these two protocols use ***120*** port number and if one one protocol is activated for transmission other one will not be activated , but manually activated once this port is idle(manual activation)

Rule2: source and destination is under two communications tcp and udp. If these two protocols use ***202*** port number and if one one protocol is activated for transmission other one will not be activated , but automatically activated once this port is idle(auto activation).

Rule3: Here both protocols will be in loop for transmission and auto system switches this port ***306*** between tcp and udp. The advantage is use of two protocols asynchronously.

Rule4: Here both protocols will be stop state and our network system will activate either one communication on port ***401*** at any given moment of time other communication will be given access by our system. The advantage is to block this port from other network communications ie third party communications.

Rule5: Here both protocols are in the stack with start stage and always third party servers cannot have the access to the port***(405)*** because this port will always shield by our network system. So at any moment of time two protocols may come into action in switch mode by system.

Final casting table for communications:

Considering the nodes {n1, n2, n3, n4, n5, n6, n7} in our network for communications internally. We assume n1, n3, n6 are the source nodes for communications and all nodes are designation nodes. The main aim of this design for communication to ignore retransmission of the packets (which are already transmitted in the dedicated path in the redirection attribute).

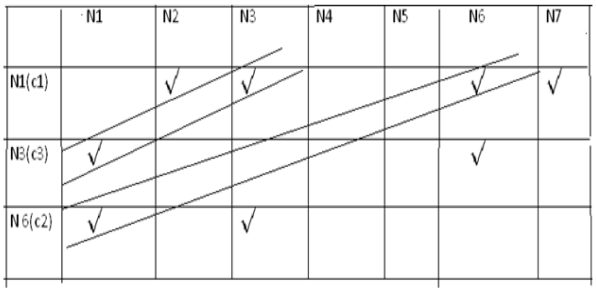
Our regular communications are below:

C1(n1 -> n2,n6,n7,n3)

C2(n6 -> n1,n3)

C3 (n3 -> n1,n6)

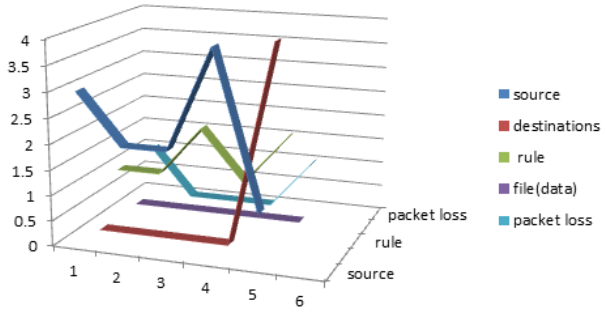
Casting table



In the above 3 cases of communcations C1 is containing n1 to n3 and C3 is containing n3 to n1, so if this communication is for same packets this communication is marked to ignore re transmission. The reason is always once the communication is done one unique identifier is generated and that identifier will activated to ignore re transmission because of marking.

Experimental result:

source	destinations	rule	file(data)	packet loss
3	8,9,10	1	PMDtest,java	1
2	11,12,13	1	callableStmt.java	0
2	12,6,9	2	AllVariety.txt	0
4	6,7,8	1	ConcreteDemo.java	0
1	4	2	MultiLive.java	1



Description:

This graph is all about the illustration of manet architecture and how the transmission takes place. It generates the source , destination nodes. Here we could observe that there is a green line which infers that certain rules are being followed along the source to destination paths. This may be from source of one network to the destination of another network.

Conclusion: Maintaining the policies of firewall at the trusted root node will grant the safety entire network tree in manet. This will give that specific path to be in a secure mode. Well this is assured by having the log maintenance which has the records of traced and untraced nodes. Moreover, we would explore how our anomaly management framework and visualization approach find out the anomalies with calculation by maintain the log in trusted nodes. In this paper we implemented the firewall anomalies reduction done in MANET only with single casting approaching.

Future work: Our future work includes usability studies to evaluate functionalities and system requirements of our policy visualization approach with MANET. Also, we would like to extend our anomaly analysis approach to reduce the anomalies by overcome the data leakages. Broad casting feature is experimental Manet can grow for more number of hops in the dynamic growth in structured network. Reduction of routers will be experimental..

Rules4-5 will be again experimental and the future challenge for multi protocols in deployments for firewalls with policy upgradation.

References

[1]Hongixin Hu,Gail-Joon Ahn,"Detecting and Resolvng Firewal Policy Anomalies,"IEEE transactions on dependable and secure computing ,
vol 9,no.3,may/june 2012.

[2] A. Wool, "Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese," IEEE Internet Computing, vol. 14, no. 4, pp. 58-65, July/Aug. 2010.

[3] J. Alfaro, N. Boulahia-Cuppens, and F. Cuppens, "Complete Analysis of Configuration Rules to Guarantee Reliable Network Security Policies," Int'l J. Information Security, vol. 7, no. 2, pp. 103-122, 2008.

[4] F. Baboescu and G. Varghese, "Fast and Scalable Conflict Detection for Packet Classifiers," Computer Networks, vol. 42, no. 6, pp. 717-735, 2003.

[5] L. Yuan, H. Chen, J. Mai, C. Chuah, Z. Su, P. Mohapatra, and C. Davis, "Fireman: A Toolkit for Firewall Modeling and Analysis," Proc. IEEE Symp. Security and Privacy, p. 15, 2006.

[6] E. Lupu and M. Sloman, "Conflicts in Policy-Based Distributed Systems Management," IEEE Trans. Software Eng., vol. 25, no. 6, pp. 852-869, Nov./Dec. 1999.

[7] I. Herman, G. Melanc¸on, and M. Marshall, "Graph Visualization and Navigation in Information Visualization: A Survey," IEEE Trans. Visualization and Computer Graphics, vol. 6, no. 1, pp. 24-43, Jan.-Mar. 2000.

[8] H.Hu, G. Ahn, and K. Kulkarni, "Anomaly Discovery and Resolution in Web Access Control Policies," Proc. 16th ACM Symp. Access Control Models and Technologies, pp. 165-174, 2011.

[9] L. Yuan, C. Chuah, and P. Mohapatra, "ProgME: Towards Programmable Network Measurement," ACM SIGCOMM Computer Comm. Rev., vol. 37, no. 4, p. 108, 2007.

[10]Bruegge, Allen H. dutiot, "Object Oriented Software Engineering: Using UML, Patterns and Java" Bernd Pearson Education pub.

[11]Herbert Schildt , "JAVA Complete Reference", TATA McGraw-Hill Edition.

[12]Bruce Eckel, "Thinking in Java", Prentice Hall

[13]Peter Coffee, Ziff-Davis Press,"How to Program Java".

[14]Miles O'Neal & Tom Stewart, M & T Books, "AWT Programming for Java".

[15] Bennett, S.S. McRobb and R. Farmer, "Object-Oriented Systems Analysis and Design usingUML". McGraw Hill, 2005 third edition.

[16]William R.Cheswick, Firewall and Internet Security,Second edition.

[17]AI-Sakib khan pathan ,Security of self organizing networks MANET,VANET ,Third edition.

.

Mr. Tatapudi Prabhakar Rao received the BTech in CSE Engg degrees from the Department of Computer Science and Engineering at GUC College Amalapuram Affiliated to Jawaharlal Nehru Technological University Hyderabad (JNTUH) and MTech in CSE Engg degrees from the Department of Computer Science and Engineering at GIET college Rajahmundry Affiliated to Jawaharlal Nehru Technological University Kakinada (JNTUK) respectively. He is currently working as Asst.Prof. in Department of Computer Science & Engineering, in Aditya Institute of Technology and Management, Tekkali, Andhra Pradesh, India. He has 8 years of experience in teaching Computer Science and Engineering related subjects. His Research interests include Image Processing, Mobile Computing, Wireless Sensor networks and Computer Forensic. He can be reached at prabhakar.tatapudi@gmail.com

Potnuru Prasanthi
M.Tech Scholar (CSE)
Aditya Institute of Technology and Management, Tekkali.

Mail id : prasanthi35@gmail.com.
Completed MCA from Aditya Institute of Technology and Management, Tekkali.