Software Defined Based Pure VPN Protocol for Preventing IP Spoofing Attacks in IOT

Narendhiran R
Department of Computer
Science and Engineering University
College of Engineering
Thirukkuvalai Nagapattinam (dt)
Tamilnadu, India
narendiranrm@gmail.com

Pavithra K
Department of Computer
Science and Engineering University
College of Engineering
Thirukkuvalai Nagapattinam (dt)
Tamilnadu, India
pavithrakdce18@gmail.com

Rakshana P
Department of Computer
Science and Engineering University
College of Engineering
Thirukkuvalai Nagapattinam (dt)
Tamilnadu, India
raxcy.98@gmail.com

Sangeetha P
Department of Computer
Science and Engineering University
College of Engineering
Thirukkuvalai Nagapattinam (dt)
Tamilnadu, India
Sangeethavanithacse2015@gmail.com

***Abstract*:-** The Internet of things (IoT) is the network of devices, vehicles, and home appliances that contain electronics, software, actuators, and connectivity which allows these things to connect, interact and exchange data. IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smart phones and tablets, to any range of traditionally dumb or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the Internet, and they can be remotely monitored and controlled. Traditionally, current internet packet delivery only depends on packet destination IP address and forward devices neglect the validation of packet's IP source address. It makes attacks can leverage this flow to launch attacks with forge IP source address so as to meet their violent purpose and avoid to be tracked. In order to reduce this threat and enhance internet accountability, many solution proposed in the inter domain and intra domain aspects. Furthermore, most of them faced with some issues hard to cope, i.e., data security, data privacy. And most importantly code cover PureVPN protocol for both inter and intra domain areas. The novel network architecture of SDN possess whole network PureVPN protocol rule instead of traditional SDN switches, which brings good opportunity to solve IP spoofing problems. However, use authentication based on key exchange between the machines on your network; something like IP Security protocol will significantly cut down on the risk of spoofing. This paper proposes a SDN based PureVPN protocol architecture, which can cover both inter and intra domain areas with encrypted format effectively than SDN devices. The PureVPN protocol scheme is significant in improving the security and privacy in SDN for IoT.

Keywords*—*IP address validation, cyber security, Pure VPN protocol, internet accountability, IP Spoofing.

*****

I. INTRODUCTION

Electric power systems are among the most important systems in our life that enable transformation of electric flow from suppliers to consumers. However, the increasing demand resulted from the growing population cannot be satisfied by the conventional electric system that has no data exchange for management or monitoring. Therefore, it was essential to enhance the infrastructure, integrating information and communication technology and improving the system security. In order to achieve these goals, the idea of smart grid has raised. Smart Grids is an enhanced electric grid with communication network on top of it, which enable the two way communication between suppliers and consumers and providing more control over the grid. It ensures the reliability and sustainability of the production and distribution of electricity through analyzing the collected information that reflects the dynamics of consumer-producer behavior.

The main objective of a Smart Grid is to utilize power resources efficiently and economically based on information gathered and data collected. Typically, a smart grid system is composed of control center, factories, smart houses, reusable energy power plants, nuclear power plants and cites. There are three major components in smart grid: control center, communication network and power grid. This project

aim at investigating the adoption of software-defined networks as a communication network replacing the legacy network and its impact on smart grid security.

Today's network must scale to accommodate increased workloads with greater agility, and keeping costs at a minimum. To meet this pressing need, software defined

networks (SDNs) has emerged as new networking paradigm based on separating control plane from data plane and centralizing the control.

SDN provides an open and programmable approach to networking through an open Application Programming Interfaces (APIs) for policy based management and security. Essentially, providing a way to automate what has traditionally been tedious manual configuration. Also, this new technology is helping with many emerging problems in networks today, such as traffic priority that cannot be treated statically as before, sometimes video traffic is more important than voice traffic and sometimes it is the other way around. However, in current networks we cannot dynamically configure traffic priority. That is when SDN comes in to play, we can dynamically model and shape traffic in real time depends on our current needs. SDN's global view of the network provides another feature via the concept of abstraction; this view hides away the distribution of the network allowing the programmer to specify the necessary forwarding behaviors without caring about vendor specific hardware and specifying objectives of overall network without caring about details of how the physical network will implement them.

This project focus on security issues of SDN-enabled smart grid systems. No doubt that implementing smart grid's communication network as a software defined network would bring several advantages in terms of security and management. However, it is important to take into consideration the threats to SDN networks in general and their impact on smart grid systems. Therefore, we investigate the resilience of POX, Floodlight and RYU SDN controllers to the following types of attacks: DoS against the controller, path congestion DoS, host location hijacking, and ARP poisoning.

II. RELATED WORKS

Pure VPN Protocol

A virtual personal network creates a virtual tunnel that extends from your device to the web server. The tunnel encrypts all the information that goes through it, thereby preventing ISPs, hackers or any entrant from viewing your activity or knowledge.

VPN Server- Connect to the worldwide network of VPN server to urge associate anonymous scientific discipline and bypass censorships and location-blocks.

VPN Client- When you got wind of and connect the VPN consumer, it mechanically creates a 256-bit encrypted tunnel for association security and privacy.

VPN Connection- Your ISP doesn't give any coding in the least, that makes your knowledge susceptible to hackers and alternative cybercriminals. By mistreatment the VPN we tend to area unit preventing ISP and also the knowledge area unit firmly changed. **IP SPOOFING**

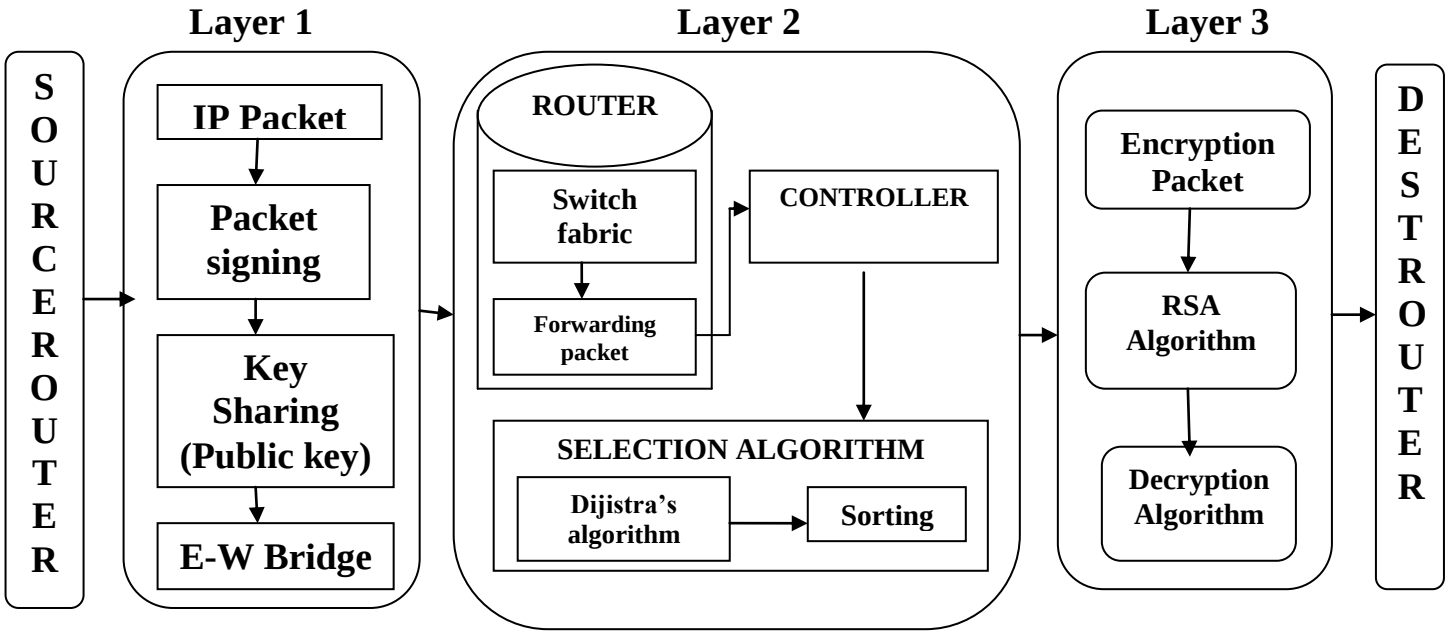
While IP spoofing used to be a much more serious and more frequently abused exploit than it is now, it is still occasionally a cause of distress for webmasters. Even though you can never be completely safe from spoofing aided attacks, there are things you can do to add a layer of protection to your site.

If you are not familiar with the term, IP spoofing denominates a practice of using different types of software to change the source or destination information in the header of the IP packets. Since these packets are sent through a connectionless network (packets in connectionless networks are also known as datagrams), they can be sent without a handshake with the recipient, which makes them convenient for manipulation. Number of ways to abuse IP or TCP spoofing (the latter mostly being a non-issue these days) kept decreasing with improvements in the overall online security, development of new protocols and increase in user awareness, but there are still people who use this for nefarious purposes. The most common abuses of IP spoofing today revolve around

- ✓ IP user authentication based exploits – where the intruder impersonates the IP of the internal network they are trying to penetrate.
- ✓ Denial-of-service attacks – either direct where the attacker modifies the destination in the IP packets, sending them to the target address; or indirect, where the attacker sends out requests to different reflectors or amplificators, with the IP's header forged so as to imply that the target site is the source of the packet. This is usually sent to a number of different reflectors / amplificators, which all reply to the target site, sometimes with a response which is much larger than the request itself.

This will prevent some of the possible exploits of IP spoofing. Ingress filtering prevents the reception of packets that are determined to be coming from a different IP address block than what is stated as the source in their header. When correctly implemented, this prevents attackers from flooding your system with requests. Egress filtering prevents packets from leaving your network, if their header seems to be tampered with, which prevents your site form being used as an amplificator or reflector.

III. SYSTEM ARCHITECTURE



LAYER 1(INTER DOMAIN):

Inter Domain- Inter Domain is that the information flow management and interaction between Primary Domain Controller (PDC) computers. this sort of laptop uses varied laptop protocols and repair to work. it's most typically wont to multicast between net domains.

IP Packet- Each packet contains a part of the message body .The networks that transfer information for all sites in little packets square measure known as packet switched networks .The packet carries information mistreatment net protocols, that is TCP/IP (Transmission management Protocol / net Protocol).

Packet signing- Packet language may be a feature through that communications exploitation SMB (Server Message Block) will be digitally signed at the packet level. Digitally language the packets allows the recipient of the packets to substantiate their purpose of origination and their credibleness.

Key Sharing (Public key) - Key exchange is any technique in scientific discipline by that scientific discipline keys square measure changed between 2 parties, permitting use of a scientific discipline algorithmic rule. If the sender and receiver would like to exchange encrypted messages, every should be equipped to write in code messages to be sent and decode messages received. the character of the mobilisation they need depends on the cryptography technique they may use. If they use a code, each would force a replica of constant codebook. If they use a cipher, they'll want acceptable keys. If the cipher may be a isobilateral key cipher each can want a replica of constant key. If Associate in Nursing uneven key cipher with the public/private key property, each can want the other's public key.

LAYER 2(SDN CONTROLLER):

SDN Controller- An SDN controller is AN application during a software-defined networking (SDN) design that manages flow control for improved network management and application performance. The SDN controller platform usually runs on a server and uses protocols to inform switches wherever to send packets.

Router-A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination node.

Switch fabric- switch fabric could be a topology within which network nodes interconnect via one or additional network switches (particularly crossbar switches). as a result of a switched material network spreads network traffic across multiple physical links, it yields higher total outturn than broadcast networks, like the first 10BASE5 version of local area network, or most wireless networks like Wi-Fi.

Forwarding packet- Packet forwarding is that the relaying of packets from one network section to a different by nodes in an exceedingly electronic network.

Dijistra's Algorithm- Dijistra's algorithmic rule (or Dijistra's Shortest Path initial algorithmic rule, SPF algorithmic rule) is AN algorithm for locating the shortest

ways between nodes in a very graph, which can represent, for instance, road networks.

Sorting- Sorting is any method of composition things consistently, and has 2 common, however distinct meanings: ordering: composition things in an exceedingly sequence ordered by some criterion; categorizing: grouping things with similar properties.

LAYER 3(PURE VPN):

Pure VPN- A virtual personal network creates a virtual tunnel that extends from your device to the web server. The tunnel encrypts all the information that goes through it, thereby preventing ISPs, hackers or any entrant from viewing your activity or knowledge.

Encryption packet- The original packet is encapsulated during a new information processing packet for transmission over the net. A SKIP or IPsec header is adscititious so the receiver will decode the packet. The secret writing method needs some artefact of the first information.

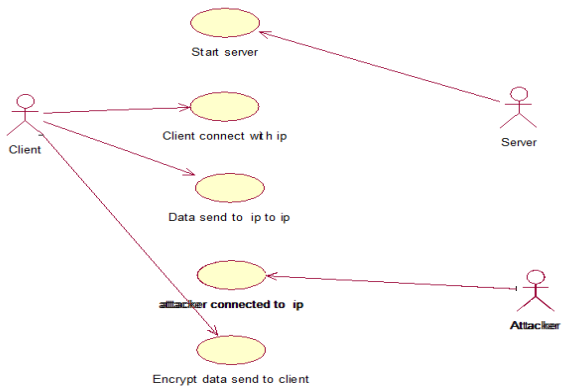
RSA algorithm- RSA is an algorithmic rule employed by trendy computers to code and decode messages. it's AN uneven cryptanalytic algorithmic rule. Uneven implies that there are 2 completely different keys. this is often additionally known as public key cryptography, as a result of one in every of the keys may be given to anyone. the opposite key should be unbroken non-public.

Decryption packet- Encryption is that the method by that a clear message is reborn to Associate in Nursing illegible kind to forestall unauthorized parties from reading it. cryptography is that the method of changing Associate in Nursing encrypted message back to its original (readable) format.

IV. SYSTEM DESIGN

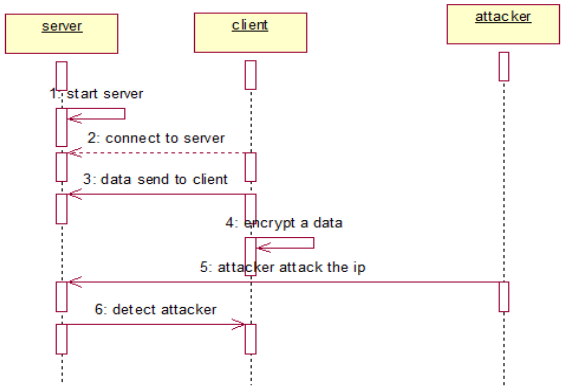
USECASE DIAGRAM

Use case diagram are usually referred to as behavior diagram used to describe a set of actions that some system should or can perform in collaboration with one or more external users of the system.



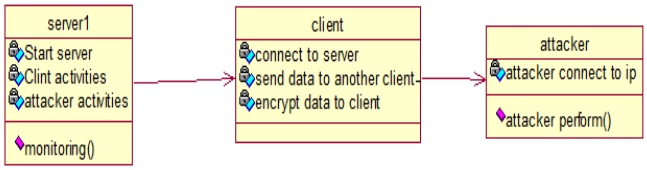
SEQUENCE DIAGRAM

A sequence diagram is an interaction diagram that shows how objects operate with one another and in what order. It is a construct of a message sequence chart. A sequence diagram shows object interactions arranged in time sequence.



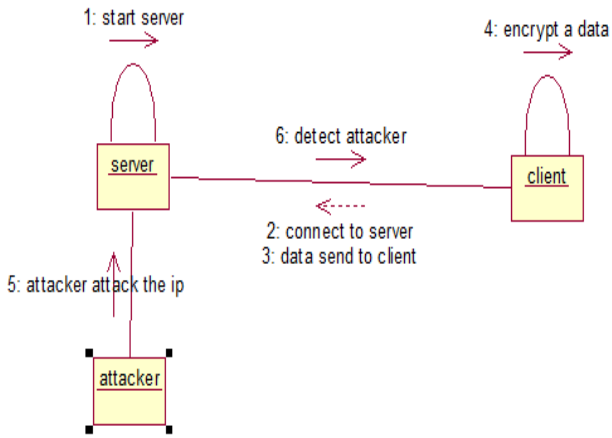
CLASS DIAGRAM

Class diagram in the unified modeling language (UML) is a type of static structure diagram that structure of a system by showing the system classes attribute operators.



COLLABRATION DIAGRAM

A collaboration diagram, also called a communication diagram or interaction diagram, is an illustration of the relationships and interactions among software objects in the Unified Modeling Language (UML). The concept is more than a decade old although it has been refined as modeling paradigms have evolved.



IMPLEMENTATION

MODULES

- Inter domain
- Detection
- Prevention

INTER DOMAIN

An inter domain packet filter (IDPF) architecture minimize the level of IP spoofing on the Internet. A key feature of this scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in Border Gateway Protocol (BGP) route updates and are deployed in network border routers. Each node only propagates and selects to neighbor based on two set of routing policies. They are import policy and export policy. The IDPFs uses a feasible path from source to the destination node, and a packet can reach to the destination through one of its upstream neighbor. Even with the partial deployment on the internet IDPF can significantly limit the spoofing capability of attackers.

DETECTION

IP spoofing is copying or making a duplicate of somebody else IP who is trusted host of the victim inside the private network. The packet filter router allows the trusted host by verifying the source IP address who is not a trusted host; attacker pretends to be trusted host. Thus an attacker enters into the private network without having an authorization.

Packet marking is the method of inserting trace-back data in to the packets which are to be traced. There are many techniques in packet marking method of IP tracing. In this paper we focusing about two methods in packet marking, DPM (deterministic packet marking) and PPM (probabilistic packet marking) both are similar kind of proposal with the minor differences.

SELECTION ALGORITHM FOR DETECTION

Input: AM, N * N topology adjacent matrix;

Output: α, proportion of SDN nodes in all nodes;

ST= Dijstra (AM) for i= 1 to N do for j = 1 to N do
$u\ all$ + =||pci ||. || pcj || end for end

for i= 1 to N
do $\beta i = ui$ / $u\ all$ end for sort (β)
for i = 1 $to\ N$ & $\lambda temp < \lambda$
do $\lambda temp$+=Distinct (βi) end for α=i/N
return

V. PREVENTION

Basically compression is classified into two types

- Lossy Compression
- Lossless Compression

LOSSY COMPRESSION

Lossy compression is a data encryption method which eliminates some of the data, in order to achieve its goal, with the result that decompressing the data yields content that is different from the original, though similar enough to be useful in some way. Lossy compression is most commonly used to compress multimedia data, audio, video, image, etc.

LOSSLESS COMPRESSION

Lossless compression is required for text and data files, such as bank records, text articles, etc. In many cases it is advantageous to make a master lossless file which can then be used to produce compressed files for different purposes.

VI. THREAT MODEL

Attack Scenarios

Also, according to the locations of spoofing source host and spoofing packets' destination, we summary the two attack scenarios that are intra-domain and inter-domain spoofing.

Intra-domain Spoofing - Intra-domain spoofing means both attacker and destination host are in the same domain, so the checkpoint in the domain border cannot effect and filter forged packets.

Inter-domain Spoofing - As various management policies exist in different ASes and routing flapping phenomenon happens occasionally between ASes, attacker could posit in any ASes and launch attack without traceback risk, which indicates deploying anti-IP-spoofing solution in inter-domain area is much difficulty than intra-domain area.

VII. PROPOSED SYSTEM

The novel network architecture of SDN based Pure VPN protocol use authentication based on key exchange on networks. It comes in the form of RSA 256-bit encryption, which is one of the most secure connections. Pure VPN provides fast speeds on high latency connections compared with SDN Controller. It is most commonly used in devices like Routers. Pure VPN protocol gives you the best speed with reliable online security. IP spoofing requires the attacker to be on the same network as you. More importantly, the attack needs some ideal conditions for it to be executed. For example, packets must be unencrypted in order to execute an IP spoofing attack. Pure VPN is the best as it can help you stay safe from the clutches of a spoof attack through its military-grade encryption. When you connect to a VPN, your data is transmitted to the ISP through an encrypted tunnel. Everything that goes through the tunnel is protected with 256-bit encryption.

RSA ALGORITHM FOR PREVENTION

Key generation algorithm,

ISSN: 2321-8169
14 - 20

INPUT: Two random prime numbers p and q.
OUTPUT: To generate public key and private key
1. Generate two large random primes, p and q, of approximately equal size such that their product n=pq is of the required bit length.
2. Compute n=pq and ϕ= (p-1) (q-1).
3. Choose an integer e, 1 < e < ϕ, such that gcd(e, ϕ)=1
4. Compute the secret exponent d, 1 < d < ϕ, such that ed ≡ 1 mod ϕ.
5. The public key is (n,e) and private key(d,p,q). Keep all the values d, p, q, and ϕ secret.

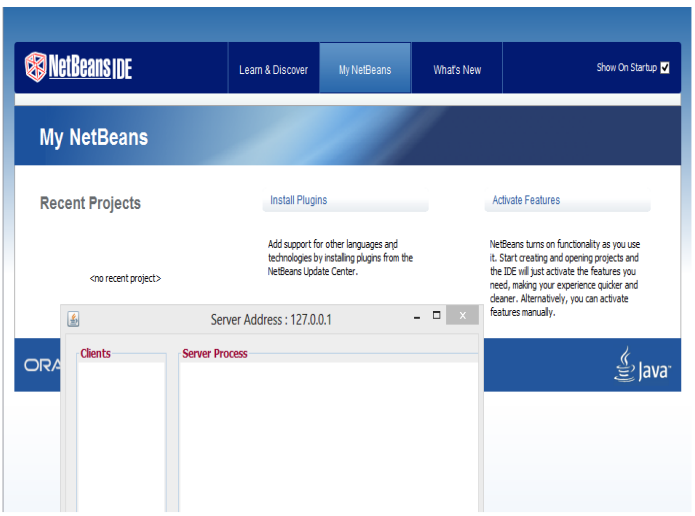
GENERATE AN RSA KEY PAIR

INPUT: Required modules bit length, k.
OUTPUT: An RSA key pair ((N,e),d) where N is the modulus,
the product of two primes (N=pq) not exceeding k bits in length;
e is the public exponent, a number less than and coprime to (p-1)(q-1); and d is private exponent i.e., ed≡1 mod (p-1)(q-1).

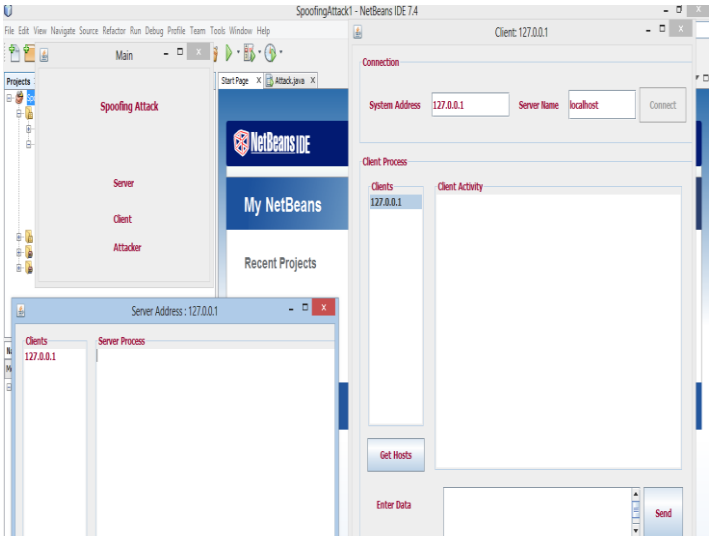
1. Select a value of e from 1 < e < ϕ
2. repeat
3. p ← genprime(k/2)
4. until (p mod e) ≠ 1
5. repeat
6. q ← genprime(k-k/2)
7. until (q mod e) ≠ 1
8. N ← pq
9. L ← (p-1)(q-1)
10. d ← modinv(e,L)
11. return (N,e,d)

VIII. OUTPUT SCREENS

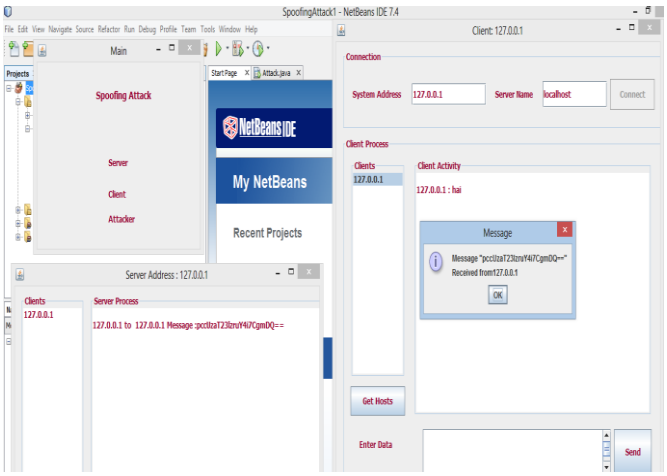
Server Activation



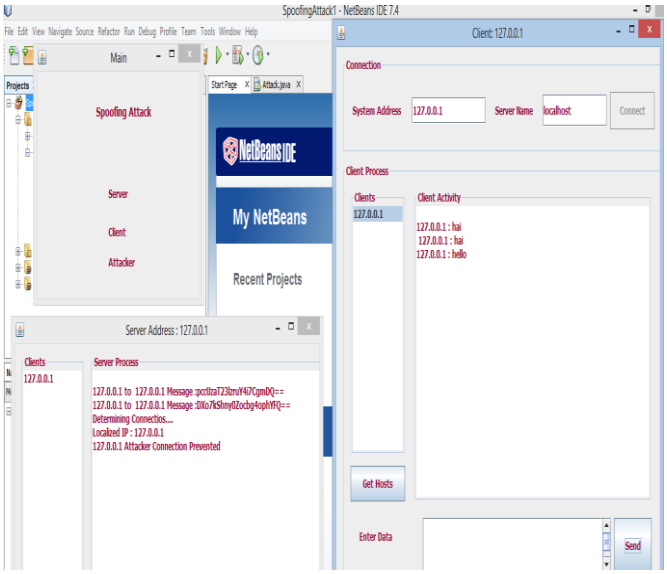
Client Activation



Message Received



Prevention of attack



IX. CONCLUSION

In our conclusion is proposed to use different trace back the source IP techniques for detecting spoofing attacks in wireless networks. Our approach can both detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that we can localize any number of attackers while logging and eliminate them. Determining the number of adversaries is a particularly challenging problem. To further improve the accuracy of determining the number of attackers present in the system. Proposed worm detection techniques to monitor and analyze the traffic in multiple locations over the Internet to detect suspicious traffic generated by worms and also examine other features of scan traffic, such as the distribution of destination addresses.

REFERENCES

[1] Amin, S. Massoud, and Bruce F. Wollenberg. "Toward a smart grid: power delivery for the 21st century." Power and energy Magazine, IEEE 3.5 (2005): 34-41.

[2] Braun, Wolfgang, and Michael Menth. "Software-Defined Networking Using Openflow: Protocols, Applications And Architectural Design Choices". Future Internet 6.2 (2014): 302-336.

[3] Kreutz, Diego, et al. "Software-defined networking: A comprehensive survey." Proceedings of the IEEE 103.1 (2015): 14-76.

[4] Craig, Alexander, et al. "Load balancing for multicast traffic in SDN using real-time link cost modification." Communications (ICC), 2015 IEEE International Conference on. IEEE, 2015.

[5] Shivayogimath, Chaitra N., and NV Uma Reddy. "MODIFICATION OF L3 LEARNING SWITCH CODE FOR FIREWALL FUNCTIONALITY IN POX CONTROLLER (WORKING ON SDN WITH MININET)."

[6] Wallner, Ryan, and Robert Cannistra. "An SDN approach: quality of service using big switchs floodlight open-source controller." Proceedings of the Asia-Pacific Advanced Network 35 (2013): 14-19.

[7] Durairajan, Ramakrishnan, Joel Sommers, and Paul Barford. "Controller-agnostic SDN debugging." Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies. ACM, 2014.

[8] H. Farhangi, "The path of the smart grid," Power and Energy Magazine, IEEE, vol. 8, no. 1, pp. 1828, January 2010

[9] Wang, Wenye, and Zhuo Lu. "Cyber security in the Smart Grid: Survey and challenges." Computer Networks 57.5 (2013): 1344-1371.

[10] Aloul, Fadi, et al. "Smart grid security: Threats, vulnerabilities and solutions." International Journal of Smart Grid and Clean Energy 1.1 (2012): 1-6.

[11] Liu, R., and A. Srivastava. "Integrated simulation to analyze the impact of cyber-attacks on the power grid." Modeling and Simulation of CyberPhysical Energy Systems (MSCPES), 2015 Workshop on. IEEE, 2015.

[12] Zhu, Kun, Lars Nordstrom, and Ahmad T. Al-Hammouri. "Examination of data delay and packet loss for wide-area monitoring and control systems." Energy Conference and Exhibition (ENERGYCON), 2012 IEEE International. IEEE, 2012.

[13] Open Netwok Foundation, "SDN Architecture Overview," version 1.0, 2013

[14] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. "OpenFlow: enabling innovation in campus networks." SIGCOMM Computer Communication Review, 38(2):6974, 2008

[15] D. Kreutz, F. Ramos, and P. Verissimo. "Towards secure and dependable software-defined networks." In Proceedings of ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN), 2013

[16] Dhawan, Mohan, et al. "SPHINX: Detecting Security Attacks in Software-Defined Networks." NDSS. 2015.

[17] Hong, Sungmin, et al. "Poisoning Network Visibility in SoftwareDefined Networks: New Attacks and Countermeasures." NDSS. 2015.

[18] Shin, Seungwon, et al. "FRESCO: Modular Composable Security Services for Software-Defined Networks." NDSS. 2013.

[19] Masoud, Mohammad Z., Yousf Jaradat, and Ismael Jannoud. "On preventing ARP poisoning attack utilizing Software Defined Network (SDN) paradigm." Applied Electrical Engineering and Computing Technologies (AEECT), 2015 IEEE Jordan Conference on. IEEE, 2015.

[20] Dong, Xinshu, et al. "Software-defined networking for smart grid resilience: Opportunities and challenges." Proceedings of the 1st ACM Workshop on Cyber-Physical System Security. ACM, 2015.

[21] Kim, Jaebeom, Fethi Filali, and Young-Bae Ko. "Trends And Potentials Of The Smart Grid Infrastructure: From ICT Sub-System To SDNEnabled Smart Grid Architecture." Mdpi.com. N.p., 2015. Web. 29 Dec. 2015

[22] Hahn, Anna, et al. "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid." Smart Grid, IEEE Transactions on 4.2 (2013): 847-855.

[23] mininet.org. "Mininet: An Instant Virtual Network On Your Laptop (Or Other PC) - Mininet." Mininet.org. N.p., 2015. Web. 29 Dec. 2015

[24] Xu, Yuzhe. "Latency and bandwidth analysis of lte for a smart grid." (2011).

[25] Shahzad, S., et al. "Conceptual model of real time infrastructure within cloud computing environment." Int. J. Comput. Networks 5 (2013): 18- 24.

[26] Germano da Silva, Eduardo, et al. "Capitalizing on SDN-based SCADA systems: An anti-eavesdropping case-study." Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on. IEEE, 2015.