International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

IDARP: ID-based Address Resolution Protocol

Imtiyaz Ahmad lone*,Jahangeer Ali,Kalimullah lone
Computer science & Engg., *Lovely Professional university* , Jalandhar
Imtiyaz.it@gmail.com
Computer science & Engg., *Lovely Professional university* , Jalandhar
Jaims7575@gmail.com
Computer science & Engg., *Lovely Professional university* , Jalandhar
Kalimullahlone@gmail.com

ABSTRACT

In this paper, security attacks in ARP are classified and logically organized/represented in a more lucid manner.ARP provides no authentication mechanism to the incoming request packets this is the reason that any client can forge an ARP message contains malicious information to poison the ARP cache of target host. There are many possible attacks on ARP which can make the communication unsecure such as man-in-the-middle (MITM), Denial of service (DOS) and cloning attack

Indexing terms

denial of service (DOS) Attacks, man-in-the-middle (MITM), Address resolution protocol (ARP)

INTRODUCTION

The Address resolution protocol is the protocol is used to map the internet protocol (IP) address into the hardware address (MAC).When the host machine wants to know a physical address for any host in the network, it broadcasts the ARP request, the host that owns the IP address sends the unicast ARP reply message to indicating its MAC address. Each host machine maintains a table called ARP cache, used to convert IP addresses into MAC addresses There are many security threats in the ARP which leads us to unsecure communication because ARP is the stateless protocol, every time a host gets an ARP reply from another host, even though it has not sent an ARP request for that reply, it accepts that ARP entry and updates its ARP cache. The process of updating the host's ARP cache with the forged entry is referred to as poisoning, in fact a malicious user can poison the ARP caches to impersonate hosts, perform MITM and DOS attacks.

PROBLEM DEFINITION

After the ARP was drafted, a subtle weakness was found.Infact Arp does not provide the authentication to the source of incoming ARP packets this is the reason that an attacker can forge an ARP message containing malicious information to poison the ARP cache of the target host.ARP is a simple protocol that it works on the following.

ARP-request, the host wants to learn the MAC address of the another host in a particular network, broadcasts the ARP request on the network "Who has IP xxx.xx.xx.xx ? tell me your MAC address mm.mm.mm.mm.mm".

ARP-reply, all the host in the particular network receive the request. The host with the given IP address will reply in a unicast ARP reply and send its MAC address to the requester.

ARP suffers from the lot of threats which leads it to insecure communication and the lonely reason for these attacks is the no authentication mechanism is used in the ARP.When the victim adds an incorrect (IP,MAC) mapping to its ARP cache, this is known as the cache poisoning or Arp spoofing. The ARP poisoning is done when the attacker sends the fake <IP,MAC> address in the response of ARP request, The ARP is stateless protocol and it accepts all the incoming ARP packets and modifies the local ARP cache.ARP poisoning attacks are often used as a part other serious attacks or we can say Arp poisoning is the base for the various attacks:

Dos attacks

An attacker can attack to victim's cache by sending the fake<IP,MAC> addresses so that every packet the sender will send will be received by the attacker instead of its real destination, In Dos attack attacker can block all the communication from the host being attacked.

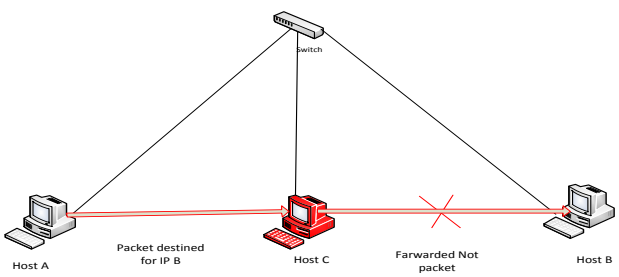


Fig. 1 Denial-of-Service (DoS) attack

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

MITM attack

The man-in-the middle attack is little different than the Dos attack, in MITM the attacker attacks two hosts at the same time by cache spoofing two hosts in the network, the attacker can silently sit between the two hosts and can read/ write the communication between two victims so that they think that they are communicating with each other, this attack is passive attack and is difficult to detect

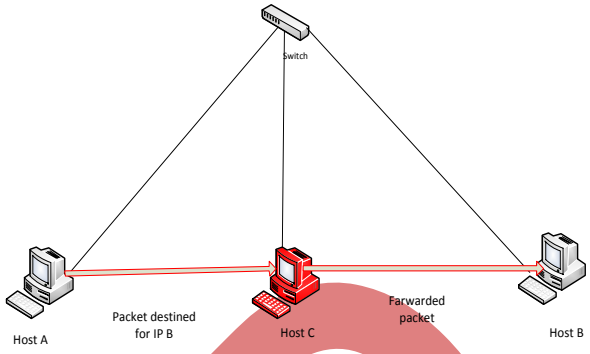


Fig. 2 Man-in-the-middle (MITM) attack

Cloning attack

The cloning attack has the different process for attacks than above two attacks, the attacker changes its IP and MAC address to become identical to those of victim host. Once the change is done there will be the two host with same addresses and victim will get confuse who is the real host and sometimes when the real host is disconnected in network the attacker can make the advantage and can attack as real host without any hesitation. This situation can cause the network troubles and we can say that it will lead to Dos attacks also.

LITERATURE REVIEW

Till present time there are many solutions for ARP-attacks to prevent the ARP-cache poisoning attacks and also provides the solution for security of ARP. Many researchers have done a good job and effort to prevent the attacks in ARP but these solutions have some drawbacks which cannot be tolerated by the network communication mechanism these solutions and their drawbacks. The drawback is that some of the solutions have no backward compatibility option and some of them use cryptography to exchange encrypted data which is not feasible because it takes too much time in encrypting the packets and few of them uses the server/middleware based solution which has the big drawback that a single crash of server can lead to failure in communication.

S-ARP: A Secure Address Resolution Protocol

D. Brusch et al. [1] proposed a solution for ARP- attack which uses the cryptography to secure the address resolution protocol. In this mechanism the sender and receiver has the private and public keys both sender and receiver uses these pair of keys to sign the message to provide the authentication and security. These keys are distributed by the third trusted party known as certification authority which helps the users in the network to provide a security mechanism. The first drawback of this mechanism is that this solution has no backward compatibility means that it takes a large cost and tough hard work to implement in the existing ARP and this solution will also lead to network conjunction because the certification authority cannot handle multiple users at a time. The second and the main drawback is that the failure of the certification authority will lead to the failure of all whole networks.

TARP: Ticket-based Address Resolution Protocol

Wesam Lootah et al. [2] proposed a Ticket- based ARP is another solution for security of ARP attacks, this solution is a well featured solution which also used the cryptography to solve the ARP threat. In this mechanism uses the ticket. Ticket-based Address Resolution Protocol (TARP). TARP implements security by distributing centrally issued secure MAC/IP address mapping attestations called tickets, are given to clients as they join the network and are subsequently distributed through existing ARP messages. Tickets authenticate the association between MAC and IP addresses through statements signed by the Local Ticket Agent (LTA).This solution suggests us to make use of cryptography for generating tickets and a server which will distribute tickets, this solution is very hard and the failure of server can fail the whole method of security, so this solution is not feasible.

A middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning

Tripunitara et al. [3] proposed a middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning attacks . Their implementation requires a “Streams based protocol stack,” but could be ported to other platforms. The proposed solution is to block unsolicited ARP replies and to raise alarms when a reply is inconsistent with the currently cached ARP entry. Implementing this scheme requires the installation of the middleware on every host on the network. The middleware was also designed to work in the presence of gratuitous ARP

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

messages and proxy ARP servers. One important limitation of this solution is that since it depends on duplicates to detect attacks, it does not prevent/detect attacks in which the host being spoofed is down or being attacked by DoS. The second limitation of this solution is that failure of the middleware can lead to the failure of trust on network.

A Hardware Approach for detecting the ARP Attack

M.M.Dessouky et al. [4] proposed one of the solutions of ARP- attacks, this solution needs the hardware approach or we can say hardware is used to detect the ARP-attacks and then these attacks can be solved after detection. There are so many tools used to detect the ARP-attacks like ARPwatch, Intrusion Detection Systems (IDSs) and ARP guard etc. These tools have the common goal to detect the ARP attack and then solve it.

ARPWATCH

With ARPwatch, the network administrator is alerted via e-mail when (IP, MAC) address pairings change. This tool is very lightweight and widely available, but it depends on the network administrator being able to differentiate between non-forged events and ARP cache poisoning attacks, and also on his ability to take appropriate and elapsed time measured when an attack occurs.

Intrusion Detection Systems (IDSs)

Intrusion Detection Systems (IDSs) like ARPwatch are usually able to detect ARP attacks and inform the administrator with the generation of an appropriate alert or alarm. The main problem with IDSs is that they end to generate a high number of wrong positives (alarms that turn out to be not part of attacks), that for them to be effective, it becomes a must for the company to put somebody in charge of dealing with these events. While IDSs are a good option for enhancing security, their ability to detect ARP.

ARP-GUARD

ARP-Guard uses a sensor-based architecture to detect several internal network attacks like ARP attacks. The management system alerts administrators in case an ARP attack is detected from the analysis of the information received from the LAN and SNMP (Simple Network Management Protocol) sensors. MAC spoofing attacks can be detected by sending an Inverse ARP (InARP) request for a MAC address.

These hardware approaches are used to deal with the detection of ARP-attacks, obviously these hardware mechanism have the capability to detect the ARP-attacks but have the big drawbacks. The failure of hardware can lead to the failure of security of ARP and this approach has no backward compatibility and cannot be implemented in the existing ARP system. To implement such type of ARP security system we have need of a hardware device in every network or in every sub network, to place the hardware device in every network can utilize a lot of cost and we have to change the hardware device after a period and hardware also requires a power to work.In short the hardware approach is very infeasible in the world of computers.

A secure address resolution protocol

Mohamed G. Gouda et al. [5] proposed architecture for resolving IP addresses into hardware addresses over an Ethernet. The architecture consists of a secure server connected to the network and two protocols used to communicate with the server: an invite-accept protocol and a request-reply protocol. The invite-accept protocol is used by hosts to register their (IP, MAC) mappings with the server. The request-reply protocol is used by hosts to obtain the MAC address of a host connected to the LAN, from the database of the secure server. Every time node has to request the sever for the invite-accept protocol and request-reply protocol for authentication and the attacker can also use of cloning attack to eavesdrop the communication between two systems. The main drawback of this solution is the whole mechanism is dependent on the sever, solution is not beneficial without sever that means that the crash of server or attack on sever can easily allow attacker to attack and also this solution is not practical because it requires change in whole mechanism of ARP so it is hard to implement and is not feasible and has no backward compatibility.

P-ARP: A novel enhanced authentication scheme for securing ARP

P Limmaneewichid et al. [6] proposed a scheme they use standard ARP request/reply packets. They only add an authentication data, in an ARP trailer. For the proposed method, so called the cryptographic trailer based authentication scheme for ARP, they make use of trailer protocol. The trailer consists of three fields that are the Magic Number, Nonce and Authentication Data. The field ‘Magic Number’ is used to distinguish whether an ARP packet carries an ARP authentication trailer. The Magic Number is a fixed constant defined as hexadecimal 0x22. It is used to distinguish whether a trailer carries the Authentication Data. The field ‘Nonce’ is an unsigned random number that is used to prevent replay attacks. Finally, the field ‘Authentication Data’ is the output of the keyed cryptographic hash function used to validate received ARP reply packets. This method provides a better solution without any hardware implementation and without middleware but has a drawback that it enlarges the packet size of the ARP request and ARP-reply and this mechanism needs the long processing system and the main drawback of the solution is that we need a secure channel to share a key between the different user to use the mechanism. The attacker can also decrypt the one-way function algorithm such as HMAC-MD5 with 128-bit keys used in this solution and can get the secret key shared between the different users.

Preventing ARP Attacks using a Fuzzy-Based Stateful ARP Cache

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

Zouheir Trabelsi et al. [7] proposed prevention mechanism is based on the use of a stateful ARP cache. When host A generates an ARP request to get the MAC address of host B, an entry is created in its stateful ARP cache, with the status of "Waiting". Host A waits for an ARP reply, within a predefined timeout. If an ARP reply comes, then host A waits another timeout in order to collect other possible ARP replies sent by other hosts in the network. Note that if host A receives more than one ARP reply, then this means that most likely more than one host has replied. Therefore, among those hosts, only one host is an honest host, which is host B. The others are probably malicious hosts, performing ARP cache poisoning attack to corrupt the ARP cache of host A. This proposed solution has less capability to detect the ARP attack because the host cannot judge exactly which one is real host and which one fake in the case of cloning attack and using of stateful cache cannot be used to prevent the ARP attacks and sometimes is is useless to detect the attack.

ES-ARP: An Efficient and Secure Address Resolution Protocol

Ataullah et al.[8] proposed one of the latest and new proposal for ARP security mechanism. The main concept of this approach is to broadcast the ARP-reply. So that in the case of ARP attack the victim may be aware about the attack. The idea of broadcasting the ARP-reply may be considered as a better solution without third trusted party but this is only a detection technique and the attack cannot be prevented by this proposed solution. The cloning attack is also possible by using the broadcasting mechanism to secure ARP, The attacker can make use of MAC spoofing attack and ES_ARP will not be capable to detect the difference between real and fake user. The broadcast storm in network is possible by broadcasting the ARP-reply which sometimes leads to the network failure and conjunction in network.

PROPOSED SOLUTION

From the above literature survey which shows that there are many security solutions for ARP but either they fully dependent on the third trust party or some of them use the secure server to distribute the cryptographic keys to encrypt the packet or message, many solutions use hardware equipment

Trusted Third party

Some solutions use third trust party to distribute cryptographic keys to encrypt the message/ packet to ensure authentication between the hosts or may used for directly authentication between host but using of third trusted party is not bad concept but the security solution should not fully dependent upon the certification authority the solution should be work better when the sever may crash.

Hardware based solutions

Many solutions has suggested to make use of hardware devices such as ARPWATCH and ARPGAURD etc to detect ARP attacks but using of the Hardware equipments require the alert administration about attack and then the administrator will try to prevent the attack. The hardware device will consume the power and we have to place the hardware devices on every network and crash of hardware device will fail all the security of ARP

Cryptographic solutions

Solutions that are based upon the cryptography make also use of secure server which helps in key distribution, the practice of using cryptography to secure ARP makes it complex than other protocols and the resolution of address will take much time in getting keys from server and then encrypting /decrypting of packet, and in case of server crash the security mechanism will not work, failure of server will lead to insecure communication and brute-force – attacks can also crack the hash function to get the security keys.

ID-Based Address Resolution Protocol

So here is now need of such solution which will be feasible and should work properly in any condition, we are introducing an new and simple security mechanism to secure ARP which is based on the unique identity of each user and these ID's will be generated by a third trusted party in the initial stage when the host will want to join the network. There are basically two important things in our proposed solution (1) ID generator (third trusted party) (2) unique identity.

ID Generator

Third trusted party will be placed in the network to secure the ARP which will do two important tasks (a) it will generate unique id for each host who will join the network and then will store this particular information (b) it will help in updating the host's ARP cache.

Unique Identity

Each user will be given the unique identity when user joins the network, the length of the ID will be 16 bits and will be added to the ARP-packet as an additional field.

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

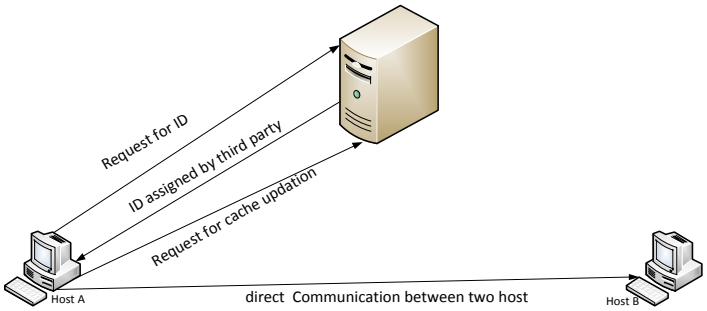


Fig1. Working of ID-Based ARP

When the host will join the network it will first register itself in the ID generator for the assignment of unique ID and update its cache. Host will first request to the third party to generate ID , third party will give it its unique ID when the host will receive the unique ID then it will send its second request to ID generator fetch recent update to update its own cache. After updating cache it will directly communicate to other host in this particular network, no broadcast request and reply is needed. The ID generator will always keep eye on the redundancy of addresses and will discard the recent redundant address if the situation will arise. By using this proposed solution attacker will never attack the communication between two hosts, if the attacker will try to perform an attack to any host the by performing the masquerade of any host, the host will check the combination of MAC address, IP address and ID, if the host will judge that the combination does not match with its existing cache information, the client will request to ID generator to update its cache again. In case of failure in third party the solution will efficiently work because ID's are given to every host until immediate recovery.

Hardware type(16 bits)	
Protocol type (16 bits)	
Length of hardware address	Length of protocol address
Operator (16 bits)	
Hardware address of sender	
Protocol address of a sender	
Unique ID of sender	
Hardware address of receiver	
Protocol address of a receiver	
Unique ID of receiver	

Table 1. New packet structure of ID-Based ARP

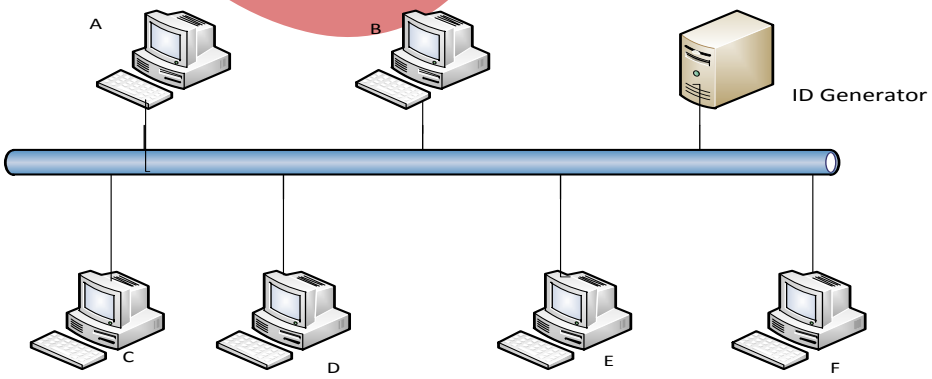
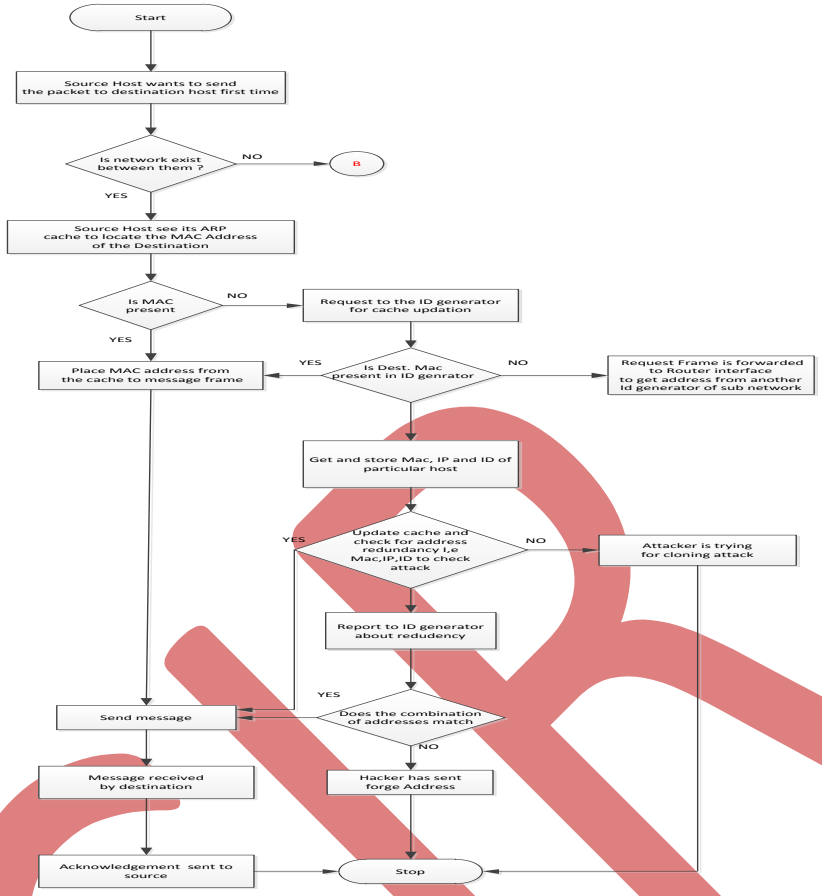


Fig 2 Architecture of ID-based ARP network

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

Flow Chart of ID-Based ARP



COMPARISON OF EXISTING SOLUTIONS

In this section we have discussed the comparison between above existing solutions, we have analysed their performance and the mechanism used for security and also the hardware equipment used for several solutions and some of them have used the cryptography mechanism to for key sharing to secure the ARP and many of them have used the third trusted party for security purpose of ARP. The below table will briefly show the different existing solutions and their performance also mechanism used.

Table 1: Requirement for different schemes, performance degradation and used mechanism for each scheme

Existing Solution	Crypto-graphy used	Hosts on network	New device added to network	Switches	Performance Degradation	Mechanism
S-ARP [1]	Yes	Trusted Host Authoritative Key	N/A	N/A	High	Signed ARP replies
TARP [2]	Yes	Trusted Host Local Ticket Agent	N/A	N/A	Low	Centrally issued tickets authenticate
Tripunitara et al.[3]	No	Special middleware	N/A	N/A	Very low	Heuristics used to block ARP
Dessouky et al. [4]	No	N/A	The HW board is connected to	N/A	No	Ping protocol to generate alarm
Gouda et al. [5]	No	Special Secure Server	N/A	N/A	N/A (replaces ARP)	Secure server resolves queries
Limmaneewichid et al[6]	Yes	N/A	N/A	N/A	Very low	Shared key is used for authentication

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

P-ARP	Yes	N/A	N/A	N/A	Very low	Different felids are added to
ES-ARP(8)	NO	N/A	N/A	N/A	Medium	ARP-reply is broadcasted at every ARP-
Proposed Solution	NO	ID generator	N?A	N?A	High	Unique ID is given to every host by ID

CONCLUSIONS

In conclusion the main aim of this paper is to differentiate between the various solutions of address resolution protocol and also discuss the limitations of these existing solutions. We analyzed several currently available solutions; identify their strengths and limitations and provide comparison among them. We have introduced a new simple and secure Address Resolution protocol which will be feasible and will make sure to secure the whole communication going between multiple hosts, no attack is possible in this type of mechanism because every user has its unique MAC,IP and ID, the ID generator will keep eye on the redundancy of addresses and attack.

REFERENCES

[1] D. Bruschi, A. Ornaghi, E. Rosti, S-ARP: a Secure Address Resolution Protocol, 1063-9527/03© 2003 IEEE

[2] W. Lootah, W. Enck and P. McDaniel, "TARP: Ticket-based address resolution protocol," in Proceedings of the 21st Annual Computer Security Applications Conference, December 2005.

[3] M. Tripunitara and P. Dutta, "A middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning," in Proceedings of the 15th Annual Computer Security Applications Conference, December 1999.

[4] M. M. Dessouky, W. Elkilany, and N. Alfishawy, "A Hardware Approach for detecting the ARP Attack," in 7th International Conference on Informatics and Systems (INFOS), May 2010.

[5] Mohamed G. Gouda and Chin-Tser Huang, "A secure address resolution protocol" in the International Journal of Computer and Telecommunications Networking, Computer Networks, Elsevier, Volume 41, Issue 1, pages: 57-71, January, 2003.

[6] P. Limmaneewichid and W. Lilakiatsakun, P-ARP: A novel enhanced authentication scheme for securing ARP, 2011 International Conference on Telecommunication Technology and Applications Proc .of CSIT vol.5 (2011) © (2011) IACSIT Press, Singapore

[7] Zouheir Trabelsi.Wassim El-Hajj,Preventing , ARP Attacks using a Fuzzy-Based

Stateful ARP Cache,1-4244-0353-7/07 ©2007 IEEE

[8] Md. Ataullah and Naveen Chauhan,ES-ARP: an Efficient and Secure Address Resolution Protocol,978-1-4673-1515-9/12 ©2012 IEEE