Research Journal of Applied Sciences, Engineering and Technology 7(23): 4872-4876, 2014
DOI:10.19026/rjaset.7.877
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2014 Maxwell Scientific Publication Corp.
Submitted: November 13, 2013 Accepted: December 04, 2013 Published: June 20, 2014

Research Article

Privacy Enhanced Pervasive Computing Model with Dynamic Trust and Security

[1]Geetha Mariappan and [2]Manjula Dhanabalachandran
[1]Department of CSE, Rajalakshmi Institute of Technology,
[2]Department of CSE, CEG, Anna University, Chennai, Tamil Nadu, India

Abstract: The objective of the research work is to propose a policy aware privacy enhancement model using dynamic trust and security management techniques. The different polices of the stakeholders incorporating device manufacturer, service provider, Mobile agents and mobile users are considered to achieve an enhanced privacy for on-demand request. The entities involving direct and indirect trust establishment with all forms of uncertainties like DDoS attacks are considered along with multiple layers of security management operations across varying trusted entities. The focus is to enhance the existing privacy through an efficient, preventive, detective, response mechanisms for those attacks, which will address the problem of DDoS before, during and after an actual attack. The session time and access time are controlled by the privileges and rights for disclosure of information in pervasive environment.

Keywords: DDoS attack, flooding, reliability, routing

INTRODUCTION

In pervasive environment, DDoS attack is the main problem in all adhoc scenario i.e.,) in MANET and in wireless sensor networks, due to this dynamic nature, to combat or trace back of DDoS attack is difficult. Zargar *et al*. (2013) In today's internet, even to protect victims large scale bandwidth, to protect target machine from heavy traffic and to avoid clogging all the routes to the victim are also difficult to implement (Anup *et al*., 2012). So, the relevant information required by the victim is not possible to receive (Sharma *et al*., 2012).

During the design of a privacy-sensitive pervasive monitoring system, the issues like Information misuse, leakage, information eavesdropping, social implications, designing privacy settings, lack of support in designing privacy-sensitive applications creeps inside the network layer and transport layer (Ramli *et al*., 2010). Also application layer be affected by internal or external system attackers if they are not follow the system protocols as per the proposal of Rongxing Lu and others, a Secure and Privacy-preserving Opportunistic Computing (SPOC) framework for m-Healthcare emergency (Lu *et al*., 2012).

In this study, we focus on DDoS attacks and the mechanisms which will address the problems of those attacks occur in pervasive environment at different layers like network layer, transport layer and application layer. In pervasive environment, constructing of Defense mechanisms with the problems of an actual attack occur before, during and after the transmission is very difficult (Al-Karkhi *et al*., 2012). So it is important to develop a new enhanced defense mechanism for handling issues related to information security for cross layer.

DDoS uncertainties: A distributed denial-of-service attack occurs if the service is denied by sending a stream of packets to trusted user after he receives request that either consumes by some botnet resources, thus it reflects it is unavailable to legitimate requested users, or provides the attacker with unlimited access to the victim machines, so that he cannot respond to the users with in a time. In hacker's society, one attacker or hacker continuously sends his attack program on insecure machine in a pervasive environment. This results, insecure machine is compromised by attack program. So, this machine is called Master/Hacker or Zombie. Collections of these machines are called bots and the corresponding network is called botnet. Through master, attacker can run their attack program on those insecure machines to launch their attacks. DDoS flooding attack and Vulnerability attack are two major categories of DDoS attacks. Only we focus on DDoS flooding attacks and their types in this study. There is various performance metrics that can be used to analyze the performance of protocols used in the pervasive environment framework. The metrics will play a significant role while analyzing performances of different environments.

Corresponding Author: Geetha Mariappan, Department of CSE, Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India
This work is licensed under a Creative Commons Attribution 4.0 International License (URL: http://creativecommons.org/licenses/by/4.0/).

Based on protocol level it is again categorized into the following.

Network/transport-level DDoS flooding attacks: These type of attacks have been launched by the protocols which are used by wired, wireless and MANETs.

Prominent attribute linkage attack: Attackers used trial and error method to find out their victim's resources by the distinguished feature of that particular scenario.

Service identity linkage attack: Attackers usually send forged request instead of requesting them directly to the service; hence those attackers can able to get victim's resources.

Un-trusted service provider attack: Attackers can able to get the details of victim's resources by providing knowingly or unknowingly through un-trusted service provider.

Service attribute linkage attack: Using attributes of particular service's Identity, Attackers can get the details of the original Identity of the service first, then it sends forged requests to the resources next.

Service status availability attack: After knowing the details of services which are available or not, attackers may attack.

Application-level DDoS attacks:

High rate request attacks: Attackers send high rate of legitimate application layer requests to a server in order to get the details of its session resources.

Service degrades attack: Instead of high rate requests to the server, it sends normal request to the server for getting high-workload response. For example, a client sends a single request to consume large amount of server resources in order to degrade the service or bring it out completely damaged.

Collaborated request attack: Attackers send high volume of requests to the server for getting high-workload responses in order to spoil the entire control of the application.

METHODOLOGY

Dynamic trust management framework: In this study we propose a dynamic trust management framework given in Fig. 1, for pervasive environment which provides the feature of defense the environment and the protection against attackers. As per the proposal of (Sharma *et al*., 2012), Intrusion detection system uses the parameters Throughput, Packet delivery Fraction, End to End delay, normalized routing load, Packet reception rate and inter arrival time to detect and avoid anomalies in MANET. These parameters are not sufficient to produce such a good result in Pervasive environment. If we add other parameters with these, will produce more accurate results. So, in our work we incorporate different parameters in pervasive environment. We assume that in our framework consists wired network with 2 or more nodes, MANET with 2 or more nodes and wireless network with 2 or more nodes which communicate with each other. According to the network, routing protocol is used and result will be analyzed with one way communication and multi-way communication.

Preventive, detective, response mechanism: Mobile Networks are considered in pervasive environment for route discovery and maintenance, three types of protocols are followed for communication. One is Proactive protocols such as Wireless Routing Protocol (WRP), Destination Sequence Distance Vector (DSDV) protocol, Fisheye State Routing (FSR), second one is reactive protocols like Dynamic Source Routing (DSR) and Ad-hoc on-demand Distance Vector routing procols (AODV), Finally hybrid protocols such as Zone Routing Protocols (ZRP), Zone-based Hierarchical Link State routing protocols (ZHLS) and Hybrid Ad-hoc Routing protocol (HARP) (Thakare and Joshi, 2010; Dhakal and Gautham, 2013; Singh and Singh, 2012).

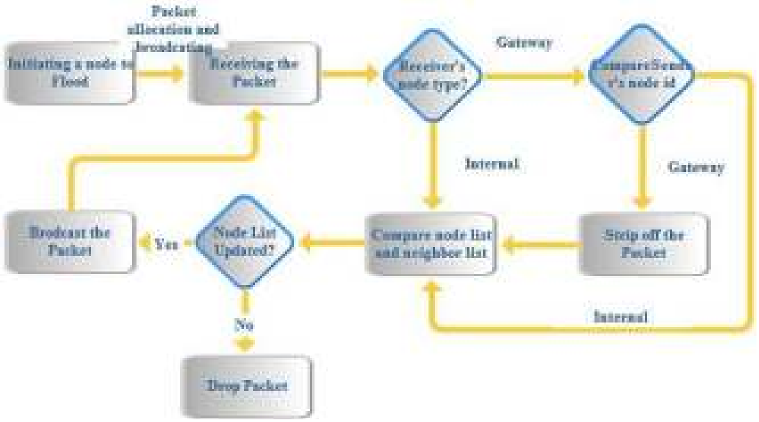

Fig. 1: Dynamic trust management framework

Overview of Ad-hoc On-demand Distance Vector routing (AODV): AODV is a reactive protocol which mixes properties of DSR and DSDV for route discovery and route maintenance as per the on-demand request from the sender. As long as routes are required, the same can be maintained after the discovery. AODV also using the following control messages like Route Request (RREQ), Route Reply (RREP), Route Error (RERR) when source is sending packets to a destination.

Route discovery process of AODV protocol can be initiated by the source to communicate to the destination, link failures or link broken. To find the destination node, route discovery process floods the RREQ messages to its neighbor. An intermediate node receives request, immediately it wants to setup reverse path to the source node with sequence number and Broadcast ID for loop free routing. When Destination receives this request, it can be replied with RREP message containing number of hops and latest sequence number. RREP is routed back to the source using reverse path and forward path from the destination. For each reverse route entry, a concept of time to live is associated and if no packets are sent within this time limit, the particular route will be removed from the routing table of concerned nodes. In route maintenance process, all nodes want to send hello message to the neighbors to confirm their links. If any of the links fails, the particular node wants to generate RERR message to its up streaming neighbors to update their routing table. After the error message received by the source, it restart the process of route discovery.

Overview of Dynamic Source Routing (DSR): It is a simple and efficient proactive protocol, based on the theory of source based routing. The route discovery process is initiated by the source node if the route doesn't know to the source. After discovery it is maintained and stored at each node's cache. During the process of maintenance, if any link failure, this process finds an alternate path to destination when source is sending packets to destination.

Reliability (single path) algorithm: The single path routing reliability algorithm is described below:

Step 1: The source node broadcasts the packet to its neighbors in the reliable path.

Step 2: The receiving node checks to see whether the packet's sequence number is already in its received list of sequence numbers.

- If so, it drops the packet.
- Else, it stores the sequence number of the packet it receives and sets its id, grid id and node type in the packet.

Step 3: If it has received from a node in the same grid, it compares its neighbor list with the node list in the packet.

- If there are nodes in the neighbor list not present in the node list, it adds those nodes to the node list and broadcasts the packet to its neighbors.
- Else, it drops the packet.

Step 4: If it has received from a node in a different grid, it strips off the node list, adds all its neighbors to the node list and broadcasts the packet.

Reliability (single path) pseudo code: The single path routing reliability algorithm for the is described below:

```
1)  Set
    tabP: Hash table of packets
    tabN: Hash table of
    neighbours
    tabNL: Hash table receive
    node list.
2)  Input: Packet[
    sID: source ID, gID: grid ID,
    seq: Sequence Number,
    nT: Node Type,
    rNL: Receiver Node List]
    If (seq) sequence number
    presents in tab P
    Return
    Create new entry
    packet (sID, seq, rNL, gID, nT).
3)  If (gID = = neighbour node
    gID)
    If (!neighbour node)
    neighbour ode not present
    in rNL add the neighbour
    node into rNL and
    broadcast the packet to its
    neighbor
    else
    Drop the packet.
4)  If (gID! = neighbour node
    gID)
    Search in rNL and add the
    all neighbour to the node list
    and broad cast the packet.
```

Reliability (multipath) algorithm: The multi-path reliability algorithm is briefed below:

Step 1: The source node broadcasts the packet to its neighbors.

Step 2: The receiving node checks to see whether the packet's sequence number is already in its received list of sequence numbers.

- If so, it drops the packet.
- Else, it stores the sequence number of the packet it receives and sets its id, grid id and node type in the packet.

Step 3: If it has received from a node in the same grid, it compares its neighbor list with the node list in the packet.

- If there are nodes in the neighbor list not present in the node list, it adds those nodes to the node list and broadcasts the packet to its neighbors.
- Else, it drops the packet.

Step 4: If it has received from a node in a different grid, it strips off the node list, adds all its neighbors to the node list and broadcasts the packet.

Step 5: For each packet it checks the packet's sequence number and repeats the same for all the paths that come either from the same grid or from a different grid.

Reliability (multipath) pseudo code: The multi-path reliability algorithm is briefed below:

```
1) Set
   tabP: Hash table of packets
   tabN: Hash table of
   neighbours
   tabNL: Hash table receives
   node list.
2) Input: Packet[
   sID: source ID,
   seq: Sequence Number,
   rNL: Receiver Node List,
   gID: grid ID,
   nT: Node Type].
3) For each (Process the packet in all path)
   If (seq) sequence number
   present in tabP
   Return
4) Create new entry
   packet (sID, seq, rNL, gID, nT)
   If (gID = = neighbour node
   gID)
   If (!neighbour node) neighbour node not
   present in rNL add the neighbour node into
   rNL and broadcast the packet to its neighbour
   else
   Drop the packet
5) If (gID! = neighbour node gID)
   Search in rNL and add all the neighbours to
   the node list and broad-cast the packet.
6) End
```

CASE STUDY

The performance evaluation of the two routing protocols AODV and DSR with extended system are carried out to improve the metric of Reliability in pervasive environment with one way communication and multi way communication to achieve the Privacy, Trust and security.

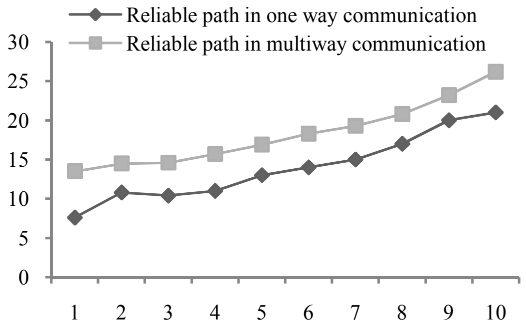

Fig. 2: Reliable paths in single and multipath communication

Table 1: Reliable paths in single, multipath communication

No of intermediate nodes	Reliable path in one way communication	Reliable path in multi way communication
1	7.6	13.5
2	10.8	14.5
3	10.4	14.6
4	11	15.7
5	13	16.9
6	14	18.3
7	15	19.3
8	17	20.8
9	20	23.2
10	21	26.2

The simulation is implemented in a Network simulator for mobile ad-hoc networks in pervasive environment. We implemented a model for checking of reliability with single path routing and multipath routing techniques. The implementation result shows that when the number of nodes increases also the number of reliable paths increases according to the result as shown in the following table.

The Table 1 and Fig. 2 describe the parameter of reliability which is measured by the number of reliable paths from the source to destination with one way and multi way communication. The following graph shows that the result of after applying prevention algorithm, the number of reliable paths increases while the number of nodes increases in both single and multi way communication. Hence the nodes can be able to sent or receive the packets in a less time because of reduction of malicious attacks and also traffic.

Through this implementation this prevention algorithm prevents the malicious attackers to exhibit the communication with less time and increased throughput through the reliability.

CONCLUSION

The techniques presented use a single path and multipath assume that the particular path is reliable, which may not hold good in reality. Link-level retransmission and Blacklisting routing use a metric to reflect and improve path reliability. Duplicate packets are not forwarded so that each node maintains a cache, which stores the signatures of recently forwarded packets and also provides the security and privacy among the transmission.

REFERENCES

Al-Karkhi, A., A. Al-Yasiri and N. Linge, 2012. Privacy, trust and identity in pervasive computing: A review of technical challenges and future research directions. Int. J. Distrib. Parallel Syst., 3: 197-218.

Anup, B., S. Amber and S.T. Satyendra, 2012. DDoS attacks impact on network traffic and its detection approach. Int. J. Comput. Appl., 40(11): 36-40.

Dhakal, D. and K. Gautham, 2013. Performance comparison of AoDV and DSR Routing protocols in mobile ad-hoc networks: A survey. Int. J. Eng. Sci. Innov. Technol. (IJESIT), 2(3): 258-265.

Lu, R., X. Lin and X. Shen, 2012. SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. IEEE T. Parall. Distr., 24(3): 614-624.

Ramli, R., N. Zakaria and P. Sumari, 2010. Privacy issues in pervasive healthcare monitoring system: A review. World Acad. Sci. Eng. Technol., 50: 741.

Sharma, P., N. Sharma and R. Singh, 2012. A secure Intrusion detection system against DDOS attack in wireless mobile Ad-hoc network. Int. J. Comput. Appl., 41(21).

Singh, G. and A. Singh, 2012. Performance evaluation of Aodv and Dsr routing protocols for Vbr Traffic for 150 nodes in manets. Int. J. Comput. Eng. Res. (IJCER), 2(5): 1583-1587.

Thakare, A.N. and M.Y. Joshi, 2010. Performance analysis of AODV and DSR routing protocols in mobile Ad hoc networks. IJCA Special Issue MANETs, 4: 211-218.

Zargar, S.T., J. Joshi and D. Tipper, 2013. A survey of defense mechanisms against Distributed Denial of Service (DDoS) flooding attacks. IEEE Commun. Surv. Tutorials, 15(4): 2046-2069.