Distributed Approach for the Security of P2P Wireless Network

Chunyong Yin[1(✉)], Nimenya Stacey[1], Tatiana Moreira Beita[1], and Jin Wang[2]

[1] School of Computer and Software, Jiangsu Engineering Center of Network Monitoring, Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology, Nanjing University of Information Science & Technology, Nanjing, China
yinchunyong@hotmail.com
[2] College of Information Engineering, Yangzhou University, Yangzhou, China

Abstract. Security for mobile P2P networks represents an open research and a main challenge regarding to their vulnerability and convenience to different security attacks such as Sybil attacks, black holes, etc. In this paper, we propose a solution based on a modification of the AODV routing protocol, taking into account the behavior of each node participating in the network solution. The benefits of our proposal are evaluated by simulation.

Keywords: P2P · Wireless mobile network · Security · Black hole · AODV

1 Introduction

In recent years, Peer-to-Peer or P2P systems have been become more and more popular, this popularity is due to the advantageous characteristics offered by such systems as: scaling, fault tolerance and control decentralized; each device can play the role of server providing such resources other nodes, a client consuming the resources of other nodes (Serve) [1]. Currently, research and industry see this model as a real alternative to the model classic client-server and contribute too many works in this field [2]. Among these, we can cite file sharing, distributed computing as well as spaces Collaboration.

The security of a wireless P2P network can be achieved at different levels of the layer protocol (Application, MAC, Routing, and Physics) and without some form of security level of one of these layers; a P2P wireless network is vulnerable to several types of attacks. It is probably fairly easy to listen to traffic, replay transmissions, manipulate packet headers, or redirect routing messages. Most of the routing protocols allow for efficient routing of data the security aspect is neglected, which also makes them vulnerable to attacks threatening reliability of the data in circulation, the question now search the optimal road but search for the most secure path.

J. J. Park et al. (eds.), *Advances in Computer Science and Ubiquitous Computing*, Lecture Notes in Electrical Engineering 474,
https://doi.org/10.1007/978-981-10-7605-3_145

2 The Proposed Protocol

The notion of trust has been applied in telecommunications with the notion of Knowledge of identities. But today the development of new Communication models such as ad hoc networks, P2P wireless networks, Vision of obsolete trust [3]. In addition, trust is not a Technical problem; it is a social problem to be opposed to the concept of security: Confidence when security is not sufficient.

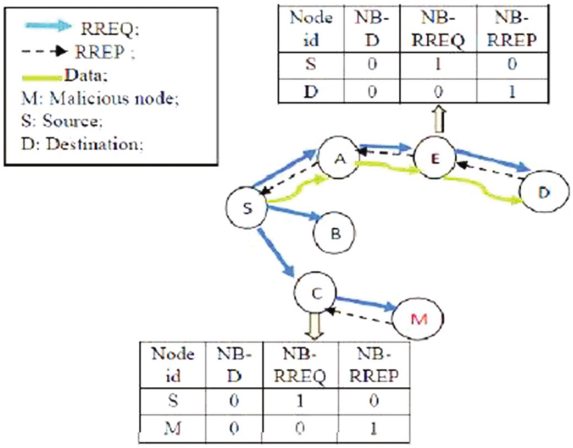

Fig. 1. Diagram depicting the detection of malicious node

We intend to propose a new protocol based on the use of a model confidence in secure P2P wireless networking in Fig. 1 while taking into account the characteristics of these networks. In our model, and in order to evaluate the degree of confidence of a node, each node in the network maintains an activity table; in this table it saves the identifier of a node, number of data packets, number of route request packets (RREQ) and the number of response packets (RREPs) received from this node. When a legitimate node receives a packet, depending on the type of packet it receives, it increases number in its activity table. If the received packet is of type RREP, it consults its activity table to check one of the equations below, depending on the values stored in this table, it decides whether the node is a node of trust or not.

Whenever a black hole node receives a data packet, it removes it directly, so when it receives a RREQ packet, it responds by sending a false RREP without consulting its routing table and it does not rebroadcast the RREQ to the other nodes. Based on this behavior, a legitimate node will not receive any data packet or A RREQ packet from a malicious node; it receives only RREP response packets, for therefore, assuming that:

NB-D: the number of data packets received from a node X
NB-RREQ: the number of RREQ packets received from a node X
NB-PAIR: the number of RREP packets received from a node X

If (D-NB + NB-RREQ > NB-PAIR) then X is a trusted node
If ((NB-D + NB-RREQ = 0) and (NB-RREP > NB-D + NB-RREQ)!) Then X is a node known
If (D-NB + NB-RREQ = 0) then X is an unknown node and can be a node Blackhole
In what follows, we present the general idea of the protocol:
Step 1:
The source node S starts the route discovery phase
Step 2:
Each intermediate node receives a RREQ stores the source sequence number (SSN)
Step 3:
When an intermediate node receives a RREP, it first checks if the node exists in the Blacklist, if the condition is true, it deletes it directly. Otherwise it goes to Step 4
Step 4:
In this step, it verifies a bit added to the format of the RREP packet, to prevent several nodes verify the same packet several times.
If (bit = 1) Then:
• The RREP was already checked by a node and the next node will not need to recheck the package (in this case the node is judged to be trusted or Known)
• RREP to the source rebroadcast
Otherwise (bit = 0)
Switch Node State
Case 1: The node is Judged Trust
Set the bit = 1
• RREP to the source rebroadcast
Case 2: The node is Judged Known
• Set the bit = 1
• RREP to the source rebroadcast
Case 3: The node is Unknown (unsecured Road, and the node can be a Black hole)
If (DSN >> SSN) (to be confirmed)
• it does not refer to the source
• Add the node to blacklist
• Remove RREP
If not
• Set the bit = 1
• RREP to the source rebroadcast
End if

3 Simulation Results

In order to implement our protocol, we used the NS2 simulation and we made several changes to several levels, first we implemented the attack, then we integrated the protocol which is a modified version of the AODV. We chose the AODV protocol because it consumes less energy, reduces the routing overhead and is more adaptable to dynamics network.

After this phase of implementation of the solution under NS2.34, we developed A TCL script [4] allowing to configure and execute the different simulations. The results of each simulation are saved in a trace file (.tr) Specified in the TCL script.

We have generated a network of 20 nodes and created a UDP connection between the nodes, we have attached the CBR (Constant Bit Rate) application that generates constant packets at Through the UDP connection. The size of the CBR packets is chosen to be 512 bytes. Time Of the scenarios is 100 s and the CBR connections start at the time equal to 1.0 s and continue until the end of the simulation, in a space of 500 × 500. Our simulations are performed using IEEE802.11 for the MAC and Random layer Waypoint Model [VASANTHI.V, 2011] as a model of node mobility. In this Last, a mobile node begins by staying in a location for a certain Time period called pause time. After this period is completed, the node moves to a randomly selected destination with a selected travel speed in the range [minspeed, maxspeed]. Once this destination is reached, it remains motionless during the specified pause time, and then repeats the process. To achieve this, NS2's ./setdest utility, which is the random generator of motion scenarios Nodes. Thus, to generate random traffic patterns, use the ./cbrgen utility.graphs by the Excel program. The table below summarizes the parameters of our experimental model (Table 1):

Table 1. Simulation parameters

Parameter	Value
Time	From 0 to 100 s
MAC	802_11
Number of nodes	20
Traffic	CBR
Pause time	2 (s)
Packet size	512 octets

In this Fig. 2 one calculates the number of data packets sent by the nodes Legitimate and received by their actual destinations. The curve of the AODV under attack is very lower than the other two.

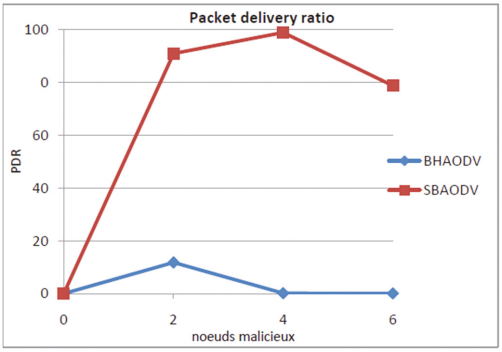

Fig. 2. PDR vs. Number of malicious nodes

Indeed, it is clear that the attacker succeeded isolate the legitimate nodes and absorb the traffic, the packets received in this case are those of nodes which are far from the malicious node, since 20 nodes have been used, if the number of nodes (to 7 for example) it has been observed that the curve of BHAODV will become 0.

4 Conclusion

In this work, we have put in place a new security protocol dedicated to P2P, which is a modified version of the AODV protocol, Is to secure the road discovery process, and thus protect the Process of transferring data based on an intrusion detection algorithm.

Acknowledgments. This work was funded by the National Natural Science Foundation of China (61772282, 61373134, and 61402234). It was also supported by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD), Postgraduate Research & Practice Innovation Program of Jiangsu Province (KYCX17_0901) and Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology (CICAEET). We declare that we do not have any conflicts of interest to this work.

References

1. Androutsellis-Theotokis, S., Spinellis, D.: A survey of peer-to-peer content distribution technologies. ACM Comput. Surv. (CSUR) **36**(4), 335–371 (2004)
2. King, R.A., Hameurlain, A., Morvan, F.: Query routing and processing in peer-to-peer data sharing systems. arXiv preprint arXiv:1005.5438 (2010)
3. Letort, V.: Adaptation du modèle de croissance GreenLab aux plantes à architecture complexe et analyse multi-échelle des relations source-puits pour l'identification paramétrique. Diss. Châtenay-Malabry, Ecole Centrale de Paris (2008)
4. Kumar, R.M., et al.: 4G–fourth generation wireless systems requirements and technical challenges. J. Theor. Appl. Inf. Technol. **31**(1), 29–35 (2011)