Cooperative Strategy to Secure Mobile P2P Network

Houda Hafi[1] and Azeddine Bilami[2]

[1] Computer science department, University of Kasdi Merbah-Ouargla-Algeria
hafi.houda@gmail.com
[2] LaSTIC Laboratory, computer science department, U.H.L-Batna-Algeria
abilami@yahoo.fr

Abstract. Mobile peer-to-peer networking (MP2P) is a relatively new paradigm compared to other wireless networks. In the last years, it has gained popularity because of its practice in applications such as file sharing over Internet in a decentralized manner. Security of mobile P2P networks represents an open research topic and a main challenge regarding to their vulnerability and convenience to different security attacks, such as black hole, Sybil...etc. In this paper, we analyze the black hole attack in mobile wireless P2P networks using AODV as routing protocol. In a black hole attack, a malicious node assumes the identity of a legitimate node, by creating forged answers with a higher sequence number, and thus forces the victim node to choose it as relay. We propose a solution based on a modification of the well-known AODV routing protocol and taking into account the behavior of each node participating in the network. Performances of our proposal are evaluated by simulation.

Keywords: Mobile wireless network, P2P, security, black hole.

1 Introduction

Traditionally, the exchange of services between computers is based on client / server model [1], this architecture has shown its limits in terms of performance, amount of processing data and network costs. The peer to peer architecture occurs as an alternative solution to the architecture client / server by providing a breakdown of traffic and load, fault resistance and anonymity. The term P2P refers to a distributed model in which entities called peers play dual role as client and server to provide to a community a service in a decentralized manner [2]. The concept behind this term is simple, its purpose is to bypass the central node in the network and to obtain a completely distributed model in which peers are considered volatile i.e. they join and leave the network unpredictably. The main consequence is the lack of confidence given to a connection between two peers. The model can be divided into three categories: centralized, hybrid or pure [3], according to the mechanism used to search and locate resources in the network. Among its many applications, we quote file sharing, distributed computing and collaborative work.

A. Amine et al. (Eds.): *Modeling Approaches and Algorithms*, SCI 488, pp. 145–154.
DOI: 10.1007/978-3-319-00560-7_19

P2P networks can be supported by wired networks as wireless networks. However, wireless P2P networks claim specific requirements in terms of security, because of their characteristics namely: unreliable links and more vulnerable to various attacks, mobile nodes powered by batteries, bandwidth much less than wired network, limited computing power. Currently very few researches have been conducted for solving security problems of wireless P2P networks; so far there are few scientific proofs on the subject. To protect the network against various malicious actions, most of these researches use traditional security mechanisms such as encryption, sealing, digital signature…

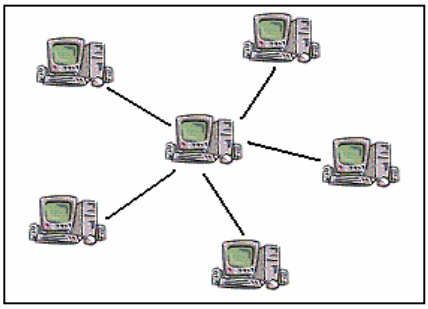

Fig. 1. Client/server model

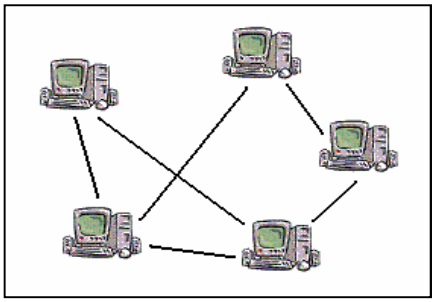

Fig. 2. Peer to Peer model

In this paper, we propose a new protocol based on the use of a trust model able to ensure the secure exchange in mobile wireless P2P networks, while taking into account the characteristics of these networks. We focus on wireless mobile ad hoc networks, where a collection of mobile entities are interconnected by a wireless technology, forming a temporary network without using any administration or any fixed support.

This paper is organized as follows, after the introduction, we present in section 2, the current state of the art of the proposed solutions described by different research teams in the literature. Our proposal is discussed in section 3. In the fourth section, we

analyze the protocol performances under different simulation conditions. Finally, we conclude with some future directions for this research.

2 Security in Wireless P2P Network

Most of security mechanisms for P2P systems are developed under the assumption of a large amount of resources, almost unlimited (CPU, memory, energy), high reliability connections through wired links, absence of node mobility, unlimited scope. For all these reasons, most of the solutions adopted in wired networks are not directly transferable to wireless P2P.

The P2P architecture is more appropriate in ad hoc environment, because it is not necessary to maintain persistent connectivity with a server; however the lack of a centralized administration makes these networks more vulnerable to different attacks. Ad hoc networks and P2P architecture share a number of similarities namely: decentralization, self-organization, the volatility (arrival and departure of nodes), the scalability and anonymity [4]. They have a relatively close structure. The security problems in both systems are similar because they have common sources and thus securing ad hoc networks especially by using distributed solutions which are not based on any central point may provide a solid approach in order to secure mobile P2P network against various malicious actions such as the Sybil attack, the Eclipse attack, Man in the middle... etc. Below we cite the main solutions currently proposed for ad hoc networks.

In [5], the authors discuss a method which mitigates the effects of black hole attack; the proposed protocol requires intermediate nodes to include information on the next hop in the RREP packet. After receiving the packet by the source node, the intermediate node sends an additional route request (FREQ) to the next node to verify that the target node (i.e. the node that just returns the RREP packet) has a route to the intermediate node and the destination. When the next hop receives a Further Request, it sends a Further Reply which includes the check result to the source node. Based on the information contained in Further Reply the source rules on the validity of the route. In this protocol, the RREP control packet is modified to contain information about the next hop. After receiving RREP, the source node sends a RREQ again to the specified node as next hop in the RREP received. Clearly, this protocol increases the routing overhead and End to end delay. Also an intermediate node must send a RREP packet twice for the same route request.

In [6] the authors have devised a new method to detect the attack black hole: it is DPRAODV "A Dynamic Learning System Against. Black hole Attack in AODV ", which tends to isolate the malicious node network. The source stores the sequence number of destination (DSN) of RREP received in the routing table and checks to see if the RREP_Seq_No is greater than the threshold value. In this protocol, the threshold value is dynamically updated at each time interval. If the value of RREP_Seq_No is found above the threshold value, the node is suspected of being malicious and is added to a blacklist. It also sends an ALARM packet to its neighbors.

The solution allows participating nodes to realize that one of their neighbors is malicious, then the node is isolated from the network and it is no longer allowed to participate in the operation of packet forwarding.

In [7], the authors describe a protocol in which the source node verifies the authenticity of a node that initiates RREP, by finding more than one route to the destination. When the source receives RREP, and if the existing routes to the destination have shared hops, the source node can then recognize a safe route to the destination.

An algorithm presented in [8] called Pre_Process_RREP, detects the black hole attack in a MANET. The Process continues to accept RREP packets and calls a process called Compare_Pkts (packet p1, packet p2), which compares the destination sequence number of the two packets and selects the packet with higher destination sequence number in case of the difference between the two numbers is not significantly high. Packet containing exceptionally high destination sequence number is suspected to be a malicious node, an ALERT message containing the node identification is broadcasted to neighbor nodes.

3 The Proposed Model

The notion of trust has been applied in telecommunications with the notion of prior knowledge of identities. But today, the development of new communication models such as ad hoc networks; mobile and wireless P2P networks make this vision of confidence obsolete [9]. In addition of that the trust is not a technical problem; it is a social problem to oppose the notion of security, we need confidence when security is not sufficient.

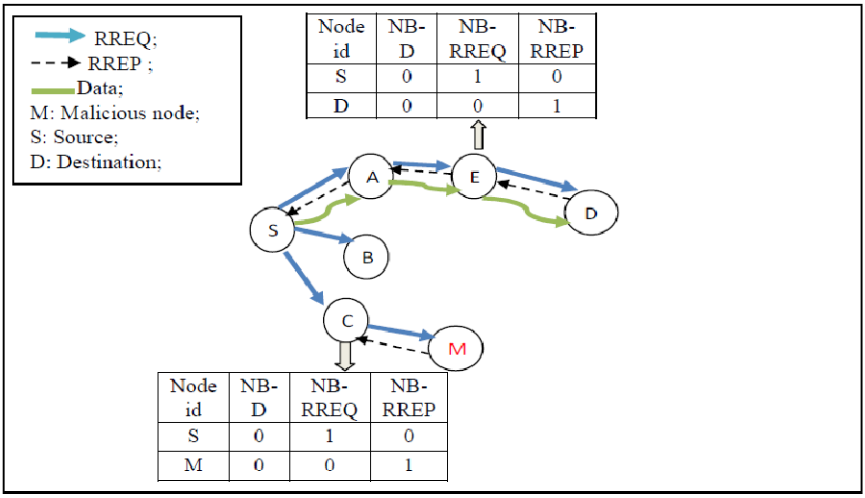

Fig. 3. Example of Diagram depicting the Detection of malicious node

In our model, in order to evaluate the node's confidence level in the network, each one maintains an activity table which stores the identifier of a node, the number of data packets, the number of route request packets (RREQ), and the number of reply packets (RREP) received from that node. When a legitimate node receives a packet (fig. 3), depending on the type of the received packet, it increases the number of received packets in the activity table. If the received packet is RREP, then it consults its activity table to check one of the following equations, based on the stored values in this table, it decides whether the node is an intruder one or not.

Whenever a black hole node receives a data packet, it deletes it directly and when it receives a RREQ packet, it responds by sending a false RREP without consulting its routing table. It avoids broadcasting the RREQ to other nodes. Based on this behavior, a legitimate node will not receive data and RREQ packet from a malicious node. It receives only the response packets.

Therefore, if we assume 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-RREP:** the number of RREP packets received from a node X

1) If **(NB-D+NB-RREQ > NB-RREP)** then: X is trusted node
2) If **((NB-D+NB-RREQ! =0) and (NB-RREP >NB-D+NB-RREQ))** then: X is known node
3) If **(NB-D+NB-RREQ=0)** then: X is unknown node and it can be a black hole node

We present below the pseudo-code of our proposed algorithm:

Step 1:
The source node S starts the route discovery process

Step 2:
Each intermediate node receives a RREQ stores the sequence number of the source (SSN)

Step 3: When an intermediate node receives a RREP, first, it checks the existence of the node in the blacklist, if the condition is true, it deletes it directly. Otherwise it goes to step 4.

Step 4: In this step it checks a bit added to the RREP packet format, to prevent that multiple nodes check several times the same packet.

```
At step 3:
If (packet==RREP) then
    If (id-node ∈ {blacklist}) then
        Delete packet
    Else
        go to step 4
    End if
End if

At Step 4:
If (bit = 1) then
        The RREP was already checked by a node and the
        next node will not need to recheck the packet,
        in this case the node is judged to be trusted
        or known (node A in figure 3).
        Rebroadcast RREP to the source.
Else (bit =0) (node E and C in figure 3)
      Switch (state of node) {
               Case 1: the node is trusted
                        Put bit = 1
                        Rebroadcast RREP to the source
               Case 2: the node is known
                        Put bit = 1
                        Rebroadcast RREP to the source
               Case 3: node is unknown (The route is
               not secure, and the node can be a black
               hole (node M in figure 3)
                       If (DSN>>SSN) (to be sure) then
                        It doesn't refer to the source
                         Add the node to the blacklist
                       End if
                              }
End if
```

Fig. 4. Pseudo code of intrusion detection algorithm

4 Simulation and Evaluation of the Proposed Approach

The implementation of malicious node behavior can be made at different levels of the protocol layer (Physical, MAC, Routing, and Application), due to different attack scenarios and vulnerabilities. In this paper a single attack on the routing layer is discussed. The implementation of malicious behavior is made on the routing layer. It can

also be made by modifying existing routing protocols such as DSR, AODV etc ... therefore; the intruder detection algorithm was also implemented in routing layer.

In order to estimate the effect of our proposal on the network level, we study the behavior of a mobile P2P network using different versions of AODV (the original AODV (without attack) and AODV with Black hole Attack "BHAODV").

To implement our protocol, we have used the NS2 simulator [10] and have made several changes at several levels; first we have implemented the attack and then have integrated the proposed protocol which is a modified version of AODV. To analyze the results, we have used awk scripts. Table 1 shows the simulation parameters used in our experiment

Table 1. Simulation parameters

Parameter	Value
Time	from 0 to 100s
MAC	802-11
Number of nodes	20
Traffic	CBR
Pause time	2(s)
Packet Size	512 octets

We measure and compare performances in terms of significant metrics such as:

- *Packet delivery ratio*: the ratio of the number of data packets received by destinations nodes to those generated by the source nodes.
- *Normalized Routing Load:* is the ratio of the number of control packets (RREQs, RREPs, and RERRs) generated by the routing protocol to the number of well received data packets.
- *Throughput:* is the amount of information transmitted per unit time.
- *The data packets received by destinations*

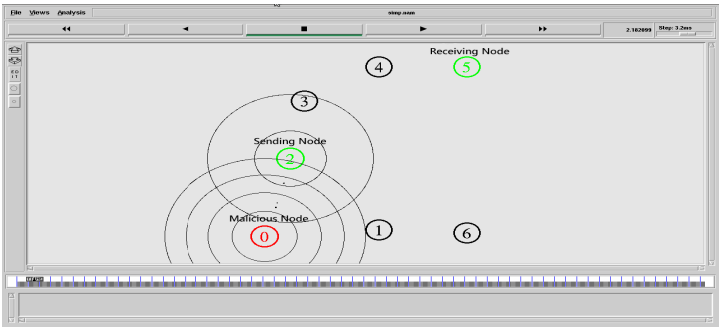

Fig. 5. Simulation of Black hole attack on mobile P2P Network under AODV

Figure 5 and figure 6 show respectively the scenario of the network simulation with the attack, and the scenario after integrating the solution. We notice in fig.6, that the malicious node has no more effect.

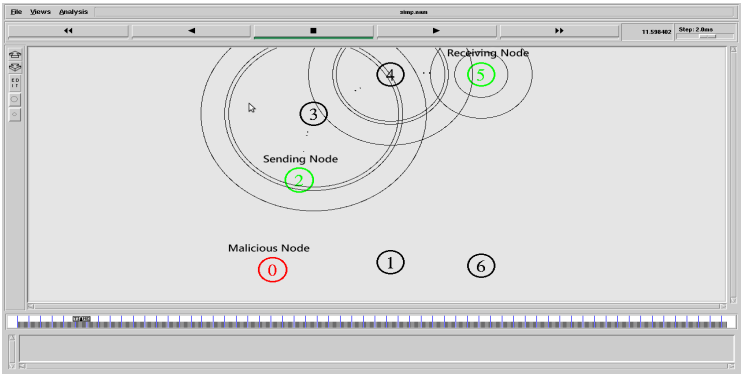

Fig. 6. Simulation of Black hole attack on mobile P2P Network under SBAODV

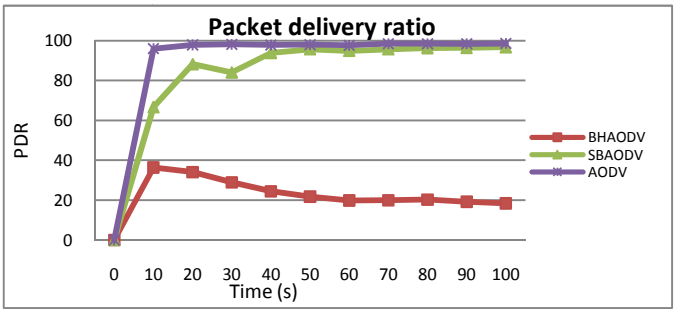

Fig. 7. Graph of Comparison Results for Packet delivery ratio

Figure 7 shows an increasing evolution of the Packet delivery ratio over time. We notice that the PDR of SBAODV after removing the attack is significantly higher than BHAODV (Black hole Attack in AODV), and becomes after a time approximately equal to AODV delivery ratio.

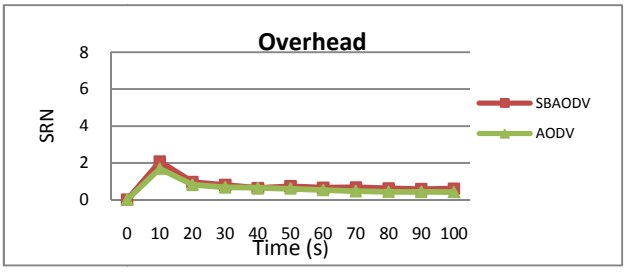

Fig. 8. Overhead using AODV and SBAODV

Figure 8 shows the routing load versus time, it is slightly more than the AODV.

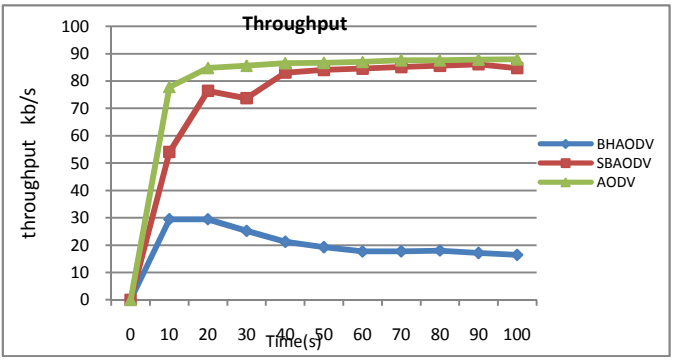

Fig. 9. Comparison Results for Throughput

Figure 9 shows the throughput versus time, for the protocol BHAODV it is very low, after the integration of our module, the throughput starts to increase gradually.

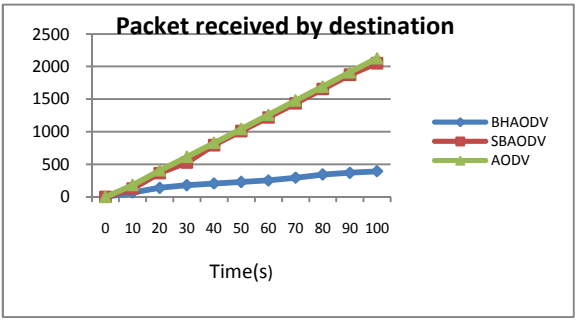

Fig. 10. The number of data packets received by destinations

In Figure 10, we calculate the number of data packets sent by the legitimate nodes and received by their actual destinations. The curve of the AODV under attack is very low compared to the others. Indeed, we clearly see that the attacker was able to isolate legitimate nodes and absorb traffic, packets received in this case are those nodes that are far from the malicious node, since we used 20 nodes, and if we reduce the number of nodes (to 7 for example), we notice that the curve of BHAODV tends to 0.

5 Conclusion

The security of mobile wireless P2P network presents a great challenge because of its autonomous and decentralized nature. Traditional security mechanisms based on the server provide an inappropriate means to protect a purely decentralized network, in such situations the distributed and cooperatives solutions are the most appropriate, because they respond suitably to the requirements of such networks.

In this work, we have implemented a new security protocol dedicated to mobile wireless P2P networks, which is a modified version of AODV protocol. The proposed mechanism tends to secure the route discovery process, and thus protects data transfer process based on an intruder detection algorithm. As a future work, we project to evaluate the capacity of our proposal to resist to other attacks under additional conditions.

References

1. Dunaytsev, R.: Client/Server and Peer-to-Peer models. Space Internetworking Center Democritus University of Thrace (2012)
2. Jarraya, H.: Un système de sauvegarde P2P sécurisé s'appuyant sur une architecture AAA, Maryline Laurent-Maknavicius (2008)
3. Shen, X., et al.: Handbook of peer to peer networking. Springer (2010)
4. Klemm, A., et al.: A Special-Purpose Peer-to-Peer File Sharing System for Mobile Ad Hoc Networks. Department of Computer Science, University of Dortmund
5. Deng, et al.: Routing "Security in Wireless Ad-hoc Networks". IEEE Communications Magazine (2002)
6. Raj, P.N., Swadas, P.B.: DPRAODV: A Dynamic Learning System Against Black hole Attack in AODV based MANET. International Journal of Computer Science (2009)
7. Shurman, M.A., Yoo, S.M., Park, S.: Black hole attack in wireless ad hoc networks. In: Proceedings of the ACM 42nd Southeast Conference (ACMSE 2004) (April 2004)
8. Mandhata, S.C., Patro, S.N.: A counter measure to Black hole attack on AODV- based Mobile Ad-Hoc Networks. International Journal of Computer & Communication Technology (IJCCT) 2(VI) (2011)
9. Véronique Legrand et Stéphane Ubéda Vers un modèle de confiance pour les objets communicants: une approche sociale, Laboratoire CITI, INRIA ARES (2004)
10. Ns-2, `http://www.isi.edu/nsnam/ns/`