CLUSTER BASED FIDELITY TO SECURE DSDV PROTOCOL AGAINST BLACK HOLE ATTACKS

Sara Boujaada, Youssef Qaraai, Said Agoujil

E3MI Team, Department of Computer Science, Sciences and Technologies Faculty, Moulay Ismail University, BP 509 Boutalamine 52000 Errachidia, Morocco.

ABSTRACT

In this paper, we introduce and discuss an approach that will be used to secure the DSDV routing protocol in an ad-hoc network. Due to mobility and absence of infrastructure, nodes are more vulnerable to several malicious attacks. The secure routing is essential to transmit packets from source to the destination. Our approach consists to model and manage fidelity concept in an ad-hoc clustering architecture. Clustering makes it possible to group the mobile nodes and to send data simultaneously to the each group. Our security model thus aims to integrate mechanisms against black hole attacks, forcing cooperation between nodes and detecting failing behaviors. The nodes present in the clusters will work more efficiently and the message passing within the nodes will also get more authenticated from the cluster heads. The simulation of our proposed algorithm is carried out using NS2 network simulator by evaluating some network performances such as average delay, throughput of communication and packets loss.

KEYWORDS

Ad-hoc, Vulnerable, Black hole attacks, Clustering, Cluster head, Fidelity, Network performance, Network Simulator.

1. INTRODUCTION

An ad-hoc network is a wireless network that is capable, to be organized without infrastructure previously defined. It is an autonomous system of mobile nodes, linked by wireless links whose union forms an arbitrary graph. Each node in the network is free to join, leave and move independently. As a result, the network topology changes instantly. To meet the need, the network may change spontaneously and configures in an autonomous way according to the existing connections between nodes. In the ad-hoc networks,

node should have the capability to function in the same time routers and terminals [1]. Moreover, the communication between nodes is ensured dynamically [2]. Routing protocols act as binding force in mobile ad-hoc and facilitate communication between nodes belonging in the network beyond the physical wireless range of the nodes [3] [4] [5]. In the hierarchical architecture nodes are divided into a number of clusters each of which is managed by a cluster head that makes control decisions for cluster members [6]. Only cluster heads nodes are participating in the routing.

The security in the routing operations represents technical challenges. Indeed, due to lack of such infrastructure or assumption of central administration, in contrast the traditional security solutions are not adapted to cope with the features of the ad-hoc networks. Several vulnerabilities exist in these networks: manufacturing, modification, selfish or malicious nodes,

DOI: 10.5121/ijans.2019.9401

usurpation of identity or suppression of the traffic in the network, the black hole attack [7], the worm hole attack [8]...

Cluster heads (CH) are responsible for monitoring all the routing activities within the cluster itself; in contrast each CH represents a point of vulnerability [9]. In particular, if no mechanism is set up to make it possible for each CH to determine the good performance and to check the coherence of the routing data, the node accepts the information of routing coming from any other node in the cluster. That is an attacker can send messages containing incorrect information on the network, in order to conduct a malicious action. For this reason, the traditional mechanisms of security and the protocols are not directly applicable and require a suitable securing in the ad-hoc networks. Several researches explored a variety of mechanisms to answer the problems of data security and a certain number of secure routing protocols have been suggested in order to prevent different types of attacks.

In this work, which is part of the security in an ad-hoc network, the routing is assumed to be provided using proactive routing protocol DSDV. In this case, we talk about an autonomous system. When the system is subject to disturbances, as the case of the black hole type, it may be that it prevents the good routing performance because of the presence of the malicious nodes. Thus, we are interested with the problem of controlling the data routed through DSDV in the presence of such a disturbance. To secure the ad-hoc networks, we envisage a clustered architecture and we will include security aspects for selection CH. Our approach named cluster based fidelity to secure DSDV protocol (CBFS) is based on the regrouping of network in clusters with each cluster is represented by a particular node called cluster head CH taking into account the level of fidelity of each node. The selected CH is responsible to manage the nodes in the same cluster and to communicate with nodes from the other Clusters.

This paper is organized as follows: In section 2 we give an overview of the DSDV routing protocol and the black hole attack. After dealing with some protocols introduced to secure DSDV protocol, we give a detailed approach followed by our proposed algorithm in the third section. The last section will be devoted to the simulation tests by considering three metrics while varying the number of black hole attacks.

2. ROUTING AND ATTACKS

2.1. DSDV Protocol

The dynamic destination-sequenced distance-vector (DSDV) is one of the proactive protocols [10]. This protocol inherits the feature and concept of Bellman-Ford algorithm and customs a table driven methodology. Each node stores a routing table containing all possible destinations with three entries: destination address, hop count and sequence number (SN). Every node i maintains for each destination x a set of distances $d_{ij}(x)$ for each node j that is a neighbor of i. Node i treats neighbor k as a next hop for a packet destined to x if $d_{ik}(x)$ equals $\min\{d_{ij}(x)\}$. The succession of next hops chosen in this manner leads to x along the shortest path. The sequence number is used to know the most recent information. So as to keep the distance estimates up to date, each node in the network monitors the cost of its outgoing links and periodically broadcasts to all of its neighbors its current estimate of the shortest distance to every other node. The distance vector which is periodically broadcasted contains one entry for each node in the network which includes the distance from the advertising node to the destination.

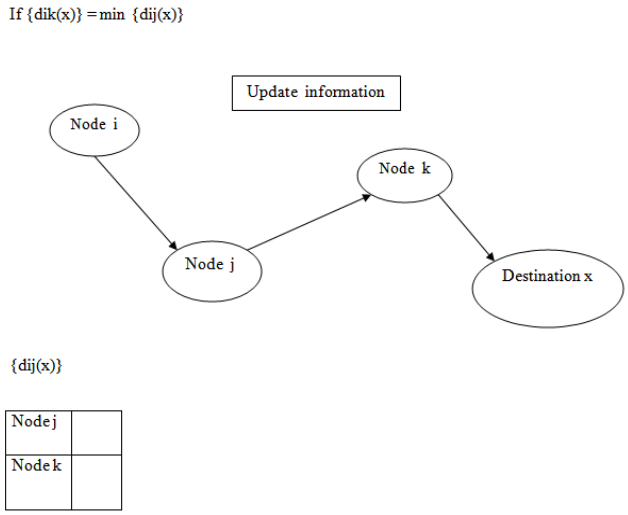

Fig.1: Illustration of DSDV

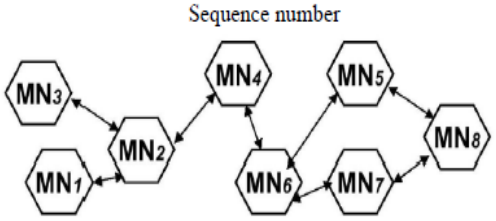

Fig.2: Example of DSDV

The DSDV initiate an interchange of routing information with its neighboring whenever a new update happens in a network. The routing updates could be sent in two ways: one is known as a "full dump", which is a packet that carries all the Information about a change and another is "incremental" will be used where only the entries that require changes are sent [11]. The nodes causes to links break when they move. When a link to the next hop is broken, the route through the next hop is assigned to infinity metric with updated sequence

number [12]. Sequence numbers assigned by the origin nodes are even numbers and to infinity metrics are odd. A node receives infinity metric, when it has an equal or later sequence number with a finite metric; it triggers to update the route, and the route with infinity metric will get replaced by a new route. When a mobile node receives new route packets then it is updated and it compares the existing with the previous in the table. DSDV updates its routing tables regularly.

2.2. Black Hole Attack

Routing protocols are having a variety of attacks in which a malicious can attract all packets by falsely claiming a fresh route to the destination and does not participate in forwarding the packets to next node; we talk about black hole attack. In other words, a malicious node uses the routing protocol (such as DSDV) to promote false information of having shortest path to the destination node or to the packet it wants to intercept, then black hole will have the accessibility in replying to the route request and creates a reply where an extremely short route is advertised.

If the malicious reply reaches node before the reply from the actual node, a forged route is created. When the attacker inserts itself between the communicating nodes, it is able to drag the packets towards them. And when the source receives these false packets, it starts transmitting the data packets to the black hole node instead of transmitting them to the destination. Below we give an extract of black hole algorithm.

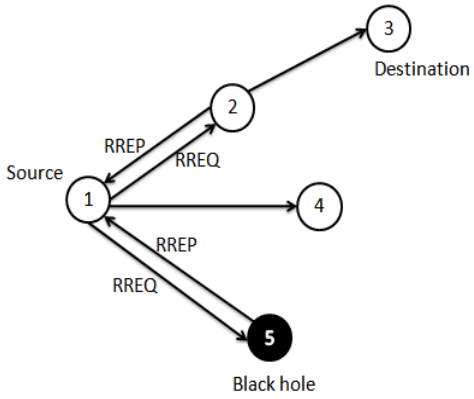

Fig.3: Example of black hole attack

Algorithm 1:

Else if ((rt and blackhole = = 1)) Then
assert (rq → rq_dst = = rt → rt_dst);
sendReverse (rq ≥ rq_src); // IP Destination
rq → rq_timestamp); // timestamp
rt → pc_insert(rt0 → rt_nexthop);
rt0 → pc_insert(rt → rt_nexthop);
Packet::free(p);
End If

3. RELATED WORKS

Security is an important research topic for mobile ad- hoc networks (MANETs), typically striving for goals like integrity to guarantee that the messages of routing exchanged between the entities were never corrupted. Authentication to verify the identity of an entity or a node in the network and the non-repudiation to verify that the sender and recipient are parties that they say have respectively sent or received the message. In recent years, there has been some proposed approaches to protect the network from black hole with the DSDV protocol.

3.1. Secured DSDV

In [13], a secure efficient ad-hoc distance vector routing protocol namely SEAD is a proactive secure ad-hoc routing protocol, based on DSDV. SEAD makes it possible to authenticate the sender of routing information, and other information provided such as the number of intermediate nodes and the sequence numbers. In order to avoid costly signatures, SEAD uses a one-way hash chain for its own entries in periodic updates, to authenticate the sequence number and metric values "hash" strings. However SEAD makes the hypothesis of a mechanism allowing a node to distribute an authentic element of the hash chain. SEAD does not regard the modification of other fields such as the next hop or the destination. It also does not protect against manufacturing and sending a new update message to another node by using the same

metric and sequence number as a recent update message. Thus, a dishonest node can modify fields that are not protected or make and inject messages where the data that will be verified are new while the rest is false.
The Secured-Destination Sequenced Distance Vector (SDSDV) [14] is a proactive secured routing protocol which aims at improving QoS requirements of the network. It uses the concept of bandwidth and Residual Energy of the node to determine the path. It uses Intruder Detection Methodology which uses threshold value and Advanced Encryption Standard (AES) algorithm for data encryption.

3.2. Clusterisation

Many clustering algorithms have been proposed in ad-hoc networks to choose cluster heads. Let's mention for example the Lowest-ID heuristic method [15] which is based on the node identifiers where each node is assigned a distinct ID and periodically broadcast the list of nodes that it capable to detect all its neighbors. The formation of clusters follows the following rules: If a node u has the lowest ID in its neighborhood, it will be selected as a cluster head. The Highest degree heuristic proposed by Gerla and Parekh [16] chooses the node having maximum number of neighbors (maximum degree) as cluster head. A node x is considered to be a neighbor of another node y if x lies within the transmission range of y. The weighted clustering algorithm (WCA) is a combined metric algorithm that uses a weighted sum of four metrics into consideration. These metrics are the degree deference D (u), the distance summation to all its neighboring nodes P(u), the mobility M(u) and the remaining battery power P(u) [6].

$$Poids\ (u) = \alpha D\ (u) + \beta P\ (u) + \gamma M\ (u) + \delta T\ (u) \qquad (1)$$

With

$$\alpha + \beta + \gamma + \delta = 1$$

4. PROPOSED APPROACH

In [17], we proposed a new method to control the AODV protocol against Black Hole attacks. It is the PC-AODV- BH protocol, a combination between the security mechanisms (digital signatures and hash functions) with the fidelity concept. In this work we will follow the same approach but in a clustering architecture in order to minimize the network load, the routing is supposed to be provided by the DSDV protocol which is the object of an black hole attack.

4.1. Description of the Proposed Architecture

The concept of security proposed in this architecture is based on the following ideas:

• Define an ad-hoc architecture based on the division of the network with a single leader (CH) by group (Cluster).

• Create an atmosphere of fidelity between all the nodes of the group; fidelity is a counter that is associated with a node, which is increased whenever it forwards a data packet successfully.

• In each group, elect a Cluster Head from among the nodes that have a smallest Poids (u) and a higher fidelity level.

• Implement cryptography to secure interactions between groups.

• Maintain security architecture as long as possible.

4.2. Clustering

In a clustering the mobile nodes are divided into several groups or substructures, called as clusters, they are allocated geographically adjacent into the same cluster according to some rules with different behaviors [18]. A typical cluster structure is shown in Fig.4. It can be seen that the nodes are divided into a number of groups (with the dotted lines) based on certain rules. Mobile nodes are classified into cluster head (CH), cluster gateway and cluster member. A cluster head normally serves as a local coordinator to manage the nodes of its own cluster and to communicate with other clusters, performing intra-cluster transmission arrangement, data forwarding, and so on. A cluster gateway is a non-cluster head node with inter-cluster links, so it can access neighboring clusters and forward information between clusters. A cluster member is usually called an ordinary node, which is a non-cluster head node without any inter-cluster links. CH is selected by basing on a specific metric or combination of metrics. Some of the parameters are residual energy, connection density and fidelity level of the node.

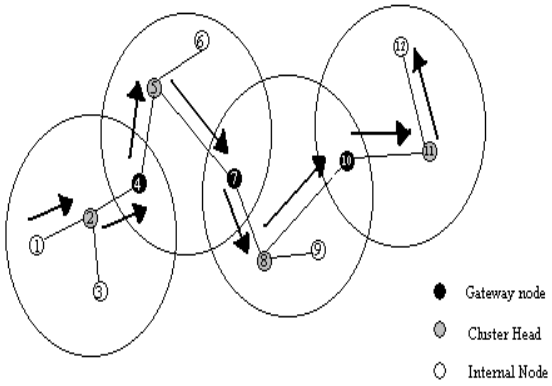

Fig.4: Cluster structure illustration

4.3. Fidelity

The proposed methodology is based on secure clustering approach for prevention of cooperative black hole attack. The proposed fidelity model is to provide the necessary mechanisms to associating a fidelity level to each node of the system via its routing table. In each node in clusters, the fidelity is basically considered as an integer number or a counter that is associated with it. This concept contributes to maintain the security of the network while measuring what one calls the fidelity levels Sara et al [17]. In other words, when the data packets are forwarded successfully, this counter is increased. According to the loyal participation of nodes in the network, their fidelity levels are updated. After successful reception of the packets by the destination node, this latter replies by sending an acknowledgement packet to the source. Fidelity level will be incremented and the packet is exchanged. If no acknowledgement is received by the source node within a timer event, the intermediate node level will be decremented and also of the next hop of the intermediate node. The fidelity tables are exchanged periodically between the participating nodes in the cluster. The fidelity level of every intermediate node i is linked to be the degree of its participation in the network operation. In other words; it is through the reports of transfer and reception of each node. Thus, the fidelity level φ_i of the node i is given by:

$$\varphi_i = \left[\frac{(MT)_i}{(MR)_i}\right]$$

Where MT (resp. MR) is the number of forward messages (resp. received) by the node i and [X] indicate the integer part of the real X.

4.4. CBFS-DSDV-BH Algorithm

In this part we present the procedure of our approach which consists of six principal steps as described in the algorithm below.

Algorithm 2:

Step1: Initialization by some parameters such as;

- x_range and y_range // x-axis and y-axis boundary.
- N // the number of nodes.
- Max_disp // maximum displacement of nodes.
- S1, S2, S3... Sn // cluster size.
- RUN_TIME // the simulation time.
- tx _range // transmission range.
- φ_i // Fidelity level.

Step2: Determination of the specific location for each node in the network.
Step3: Computation of the distance between any node and others lying in the same transmission range.
Step4: Cluster head (CH) election procedure

- Calculating degree of every node d(u). CH is selected based on the node with maximum number of neighbors in the same transmission range;
- Compute the degree difference for each node;
- Compute the speed for every node till current time T.

$$M_u = \frac{1}{T}\sum_{t=1}^{T}\sqrt{(X_t - X_{t-1})^2 + (Y_t - Y_{t-1})^2}$$

- Calculate energy of every node;
- Determinate the combined weight for every node;

$$W(u) = \alpha D(u) + \beta P(u) + \gamma M(u) + \delta T(u)$$

Step5: Integration of the fidelity concept associated with the nodes in each cluster.

- $\text{int } \varphi = \left[\frac{mt}{mr}\right]$;
- Select the node with maximum φ as a cluster head.
- for n=1:N .
  If (φ of a CH == 0)) then
  remove the CH from neighbor table and fidelity table
  Update CH election
  end

end

- Take the node with the smallest W(u) and a higher fidelity level φ_{max} as the cluster head CH

Step6: Update the node position (the entire nodes move randomly after some unit time).

Whenever we observe that the fidelity value of a particular node is greater that of another node then we can conclude that the one having the greater value is a more durable node than the other from who's its value is greater. It is quite logical because a node with greater value indicates that it is an experienced node in the network and it has transmitted packets most dutifully than other nodes and it will be selected as a CH in cluster. In the case where the level of CH or any node in cluster drops to 0, it is considered to be a malicious node, termed as a "black hole" and it is eliminated, a new election of cluster head will be made. The detection of a black hole has to be intimated to the other participating nodes in clusters. This is accomplished by sending alarm packets. When a node receives an alarm packet, it will identify the black hole and so can eliminate the use of that node from then on.

5. SIMULATIONS

Performance Evaluation

To illustrate our proposed approach, we will test the CBFS-DSDV-BH Algorithm on an example of an ad-hoc network according to three metrics using NS simulator. The number of network nodes is fixed in 42 which move in an area of 1440m*1440m. We use a CBR application (Constant Bit Rate) where the traffic between nodes is produced using a traffic generator which creates randomly CBR connections that start at moments which are uniformly distributed between 0 and 10 seconds (with a pause time equal to 1 second). The size of the transferred data is assumed to be equal to 512 bytes. The simulation parameters are summarized in table 1 below.

Before presenting the performance results of the considered network, we present in the fig.5 the simulation scenario obtained using equation (1) where the four parameters are given by: α = 0.45, β = 0.05, γ = 0.45 and δ = 0.05.

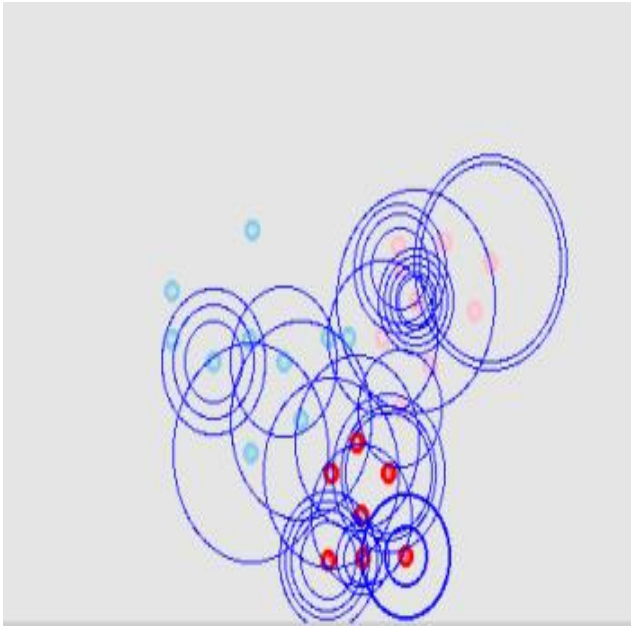

Fig.5: The proposed cluster architecture

Table 1: Simulation parameters

Parameter	***Value***
Simulator	NS2
Number of Nodes	42 nodes
Traffic Type	Constant Bit Ratio CBR
Transmission rang	250m
Terrain area	1440m*1440m
Simulation Time	10 seconds
Packet Size	512 bytes
Routing Protocols	DSDV
Pause Time	1 seconds

In order to evaluate the performance of concerned routing protocol, we recall these three definitions.

1) Average Delay: the average delay is defined as the time difference between the sending data packets by the source and the receiving data packets by the destination node.

$$AD = \frac{1}{n}\left(\sum_{i=0}^{n} PktRecvdTime - PktSentTime\right)$$

2) Throughput: is the average of successful messages delivered to the destination by a communication channel according to a given time interval

$$Throughput = \frac{\sum_{i=0}^{n} PktsRecvd * PktSize}{1000}$$

3) Packets loss: it is the difference between the amount of generated and received packets during a time of communication.

The variation of these three metrics is given according to time, and they are related to the autonomous, disturbed and controlled cases of the DSDV routing protocol state.

Autonomous system: From the table 1, the performance evaluation of the network according to the three metric ones above, while using the routing protocol DSDV, gave the following results (figs 6, 7 and 8).

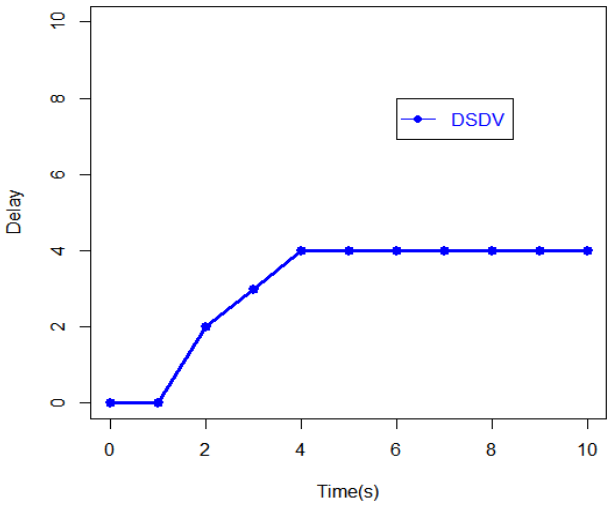

Fig.6: Average delay

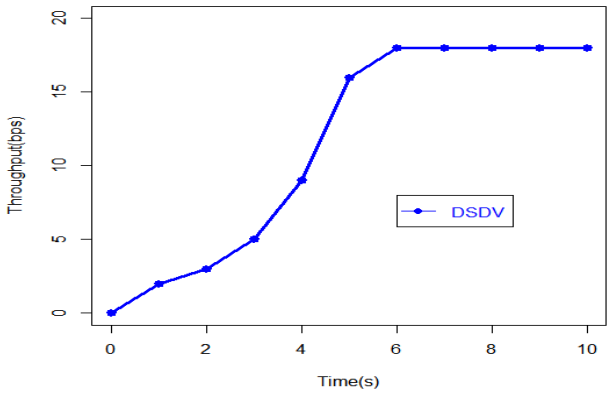

Fig.7: Throughput of communication

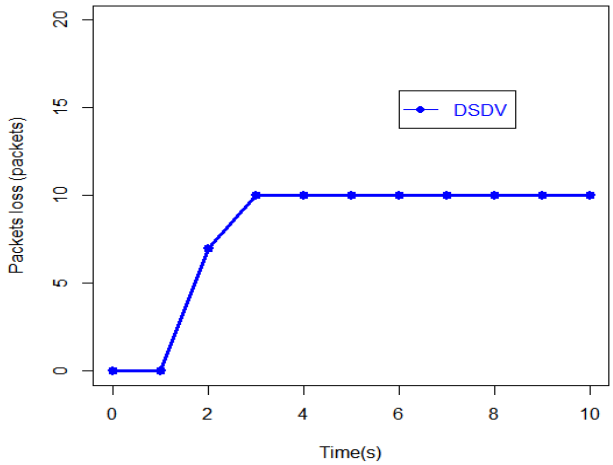

Fig.8: Packets loss

Disturbed system: Now, we assume that the network described in the table 1 is vulnerable because of the black hole attacks. In order to describe the impact of malicious nodes on the behavior of the DSDV routing, we consider two situations of black hole attack: 1 and 3. Thus we obtain the figs 9, 10 and 11.

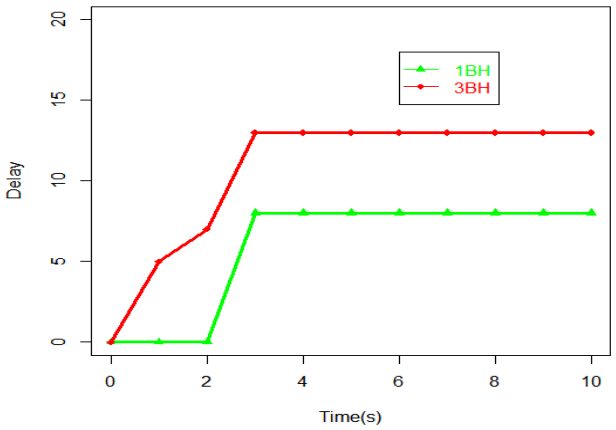

Fig.9: Average delay with black hole attacks

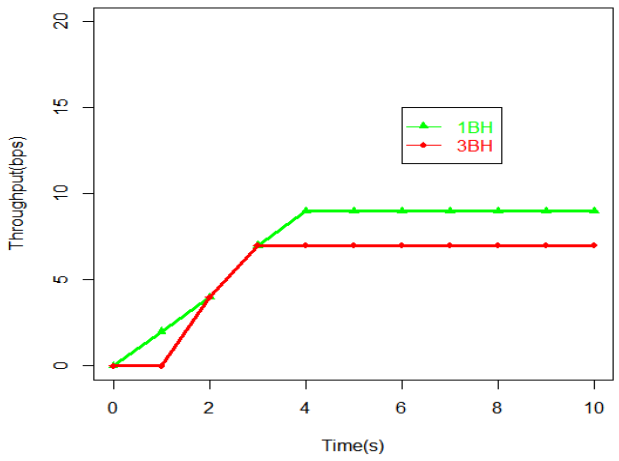

Fig.10: Throughput of communication with black hole Attacks

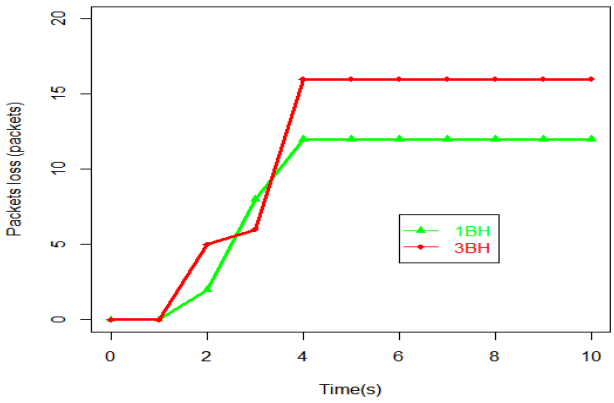

Fig.11: Packets loss with black hole attacks

Controlled system: When the network described in table 1 undergoes a disturbance of the type 1 or 3 black holes, our objective is to be able to cancel their effects using the fidelity level in clustering architecture, and then to compare in terms of effectiveness of safety of DSDV routing deal with such threats. Therefore, an implementation of the two protocols enables us to obtain the figs 12 - 17.

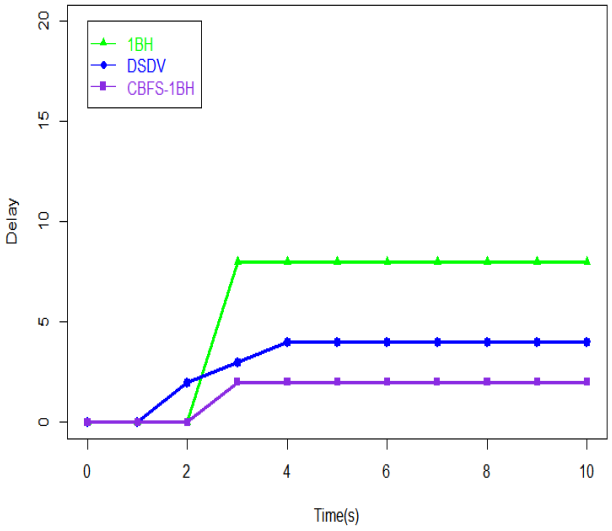

Fig.9: Average delay with black hole attacks

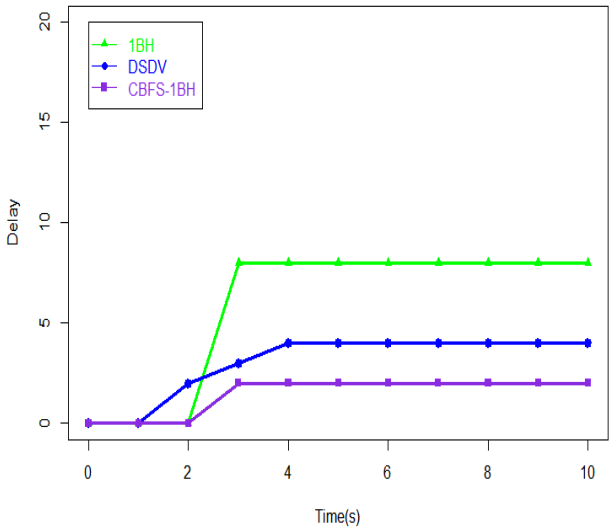

Fig.12: Controlled average delay with one black hole

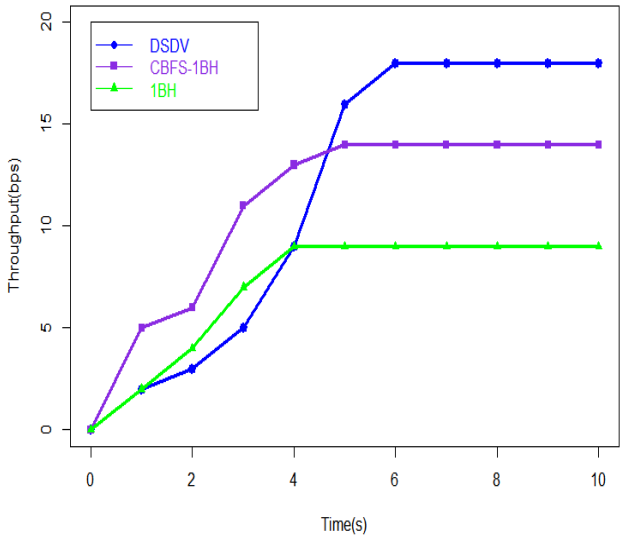

Fig.13: Controlled throughput of communication with one black hole

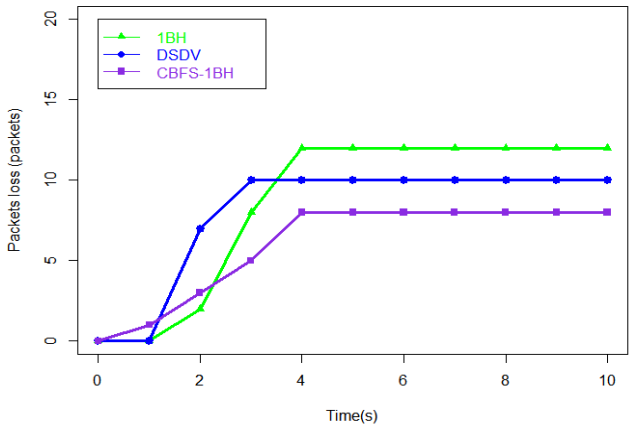

Fig.14: Controlled packets loss with one black hole

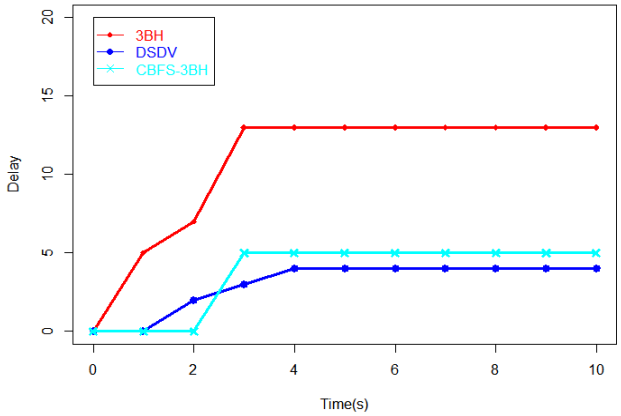

Fig.15: Controlled average delay with three black holes Attacks

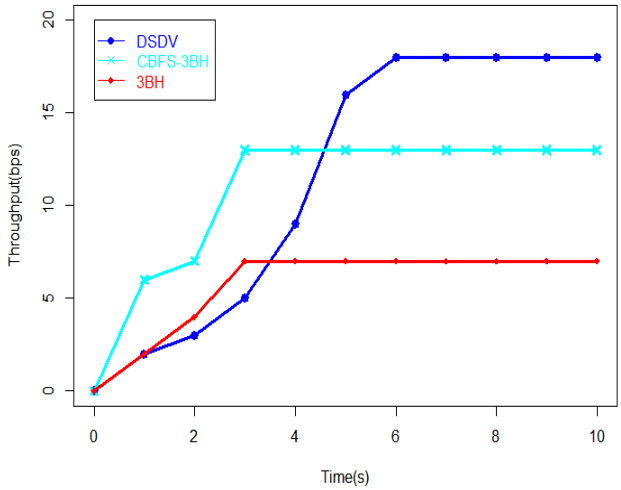

Fig.16: Controlled throughput of communication with three black hole attacks

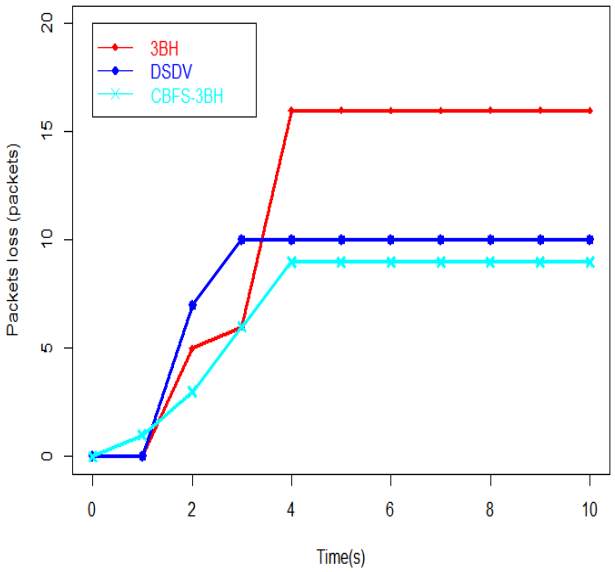

Fig.17: Controlled packets loss with three black hole Attacks

Discussion results: The figures 6, 7 and 8 represent respectively the variation, according to the time, of the average delay, the throughput of communication and the quantity of packages lost in the DSDV routing protocol. It is about a normal evolution of this protocol, because what concerns us is the control of this protocol facing the black hole attacks**.**

In the presence of this kind of attack, the behavior of DSDV is modified. Indeed, the figure 9 shows that the average delay is proportional to the number of black hole attacks over the entire interval of time. As this metric is a major challenge which any ad-hoc network seeks to minimize, its increase based on malicious nodes is due to the cooperation of the latter for the degradation of the receptions in the entire network. In a similar way, the increase in the quantity of the packets loss, figure 11 is mainly the result of the black hole attack which consists in falsifying the borrowed routes and the cooperation of the attackers as well.

The figure 10 shows the effect of black holes attacks on the throughput of communication in the network. The observed decrease is due to the fact that the bandwidth is also shared by malicious nodes that cooperate and contribute to the transfer and the reception of the data by emulating the source by erroneous information.

The objective of our approach is to be able to make the disturbed system in its autonomous state by using an protector control. From the figures 12 - 17, we note that the curves obtained by the implementation of the improved version of DSDV: Cluster Based Fidelity to Secure DSDV (CBFS) is approximately close to those corresponding to the case of the routing DSDV in the autonomous case. In other words, these one is not only made it possible to decrease the average delay and packets loss, but increased the throughput of communication. The improved version of DSDV protocol (CBFS) remain effective for the protection of the DSDV protocol against black hole attacks, since malicious nodes share the channel or bandwidth with other nodes in the network.

That being, one notes that the protocol of control is able to defend the routing in the two situations of attacks (1 and 3 black holes), for the considered metric. Moreover, the figures 12 - 17 show that our proposed scheme CBFS is approximately close to the DSDV protocol, and it’s appear efficient to secure this protocol. That is a consequence of the use of the fidelity levels and an optimal CH in each cluster for choosing the safest route

6. CONCLUSIONS

In the mobile ad-hoc networks, there is a big problem of the presence of a malicious node. In this project, we have proposed an algorithm to secure the DSDV routing protocol against black hole attacks in an ad-hoc mobile network. Our proposed approach consists in combining the clustering technique with a fidelity concept. The election of node control is made taking into account the maximum value of degree's nodes in the network. This control node is considered as the cluster head (CH) one. By consequence, the secure communication between clusters is answered by applying the routing DSDV protocol using the CH nodes.

The implementation of the resulting algorithm under NS simulator, according to the end to end delay, throughput of communication and packets loss, has shown that the proposed method made it possible to answer the objective of this work.

In the rest of this work, we intend to extend these results by comparing them with other existing secure variants of DSDV such as SDSDV, SEAD ... On the other hand, a hybrid security approach will be considered by combining the routing protocols AODV (reactive) and DSDV (proactive).

REFERENCES

[1] P. Tomar V. Sejwar P. Suman, D. Bisen and R. Shukla. Comparative study of routing protocols for mobile ad-hoc networks. International Journal of Information Technology and Knowledge Management, 2009.

[2] Chlamtac I Conti M and Liu JJ. Mobile ad-hoc networking: imperatives and challenges. ad-hoc Networks, 2003.

[3] Jasvinder and Monika Sachdeva. A survey of behavior of manet routing protocols under black hole attack. International Journal of Advanced Research in Computer Science and Software Engineering, 2013.

[4] Biradar R and Patil V. Classification and comparison of routing techniques in wireless ad-hoc networks. In ad-hoc and Ubiquitous Computing. ISAUHC06. International Symposium, page pages 712, 2006.

[5] P. Chenna Reddy and P ChandraSekhar Reddy. Performance analysis of adhoc network routing protocols. In ad-hoc and Ubiquitous Computing. ISAUHC 06. International Symposium, page pages 186187, 2006.

[6] Chatterjee M and Turgut D Das SK. Wca: a weighted clustering algorithm for mobile ad hoc networks. Journal of Cluster Computing, 05(02):193–204, 2002.

[7] S. Sharma and R. Gupta. Simulation study of blackhole attack in the mobile ad-hoc networks. Journal of Engineering Science and Technology, 4(2):243–250, 2009.

[8] Amos J Paul and Vishnu K. Detection and removal of cooperative black/gray hole attack in mobile adhoc networks. International Journal of Computer Applications (ISSN NO. 0975 - 8887), 1(22), (2010).

[9] P. S. Mann Harmanpreet Kaur. Prevention of black hole attack in manets using clustering based dsr protocol. IJCST, 2014.

[10] C.E. Perkins and E.M. Royer. : Ad-hoc on-demand distance vector routing. In: Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, page 90–100, (1997).

[11] G.Vijaya Kumar and Dr.M.Nagendra Y.Vasudeva Reddyr. Current research work on routing protocols for manet: A literature survey. International Journal on Computer Science and Engineering, Vol. 02(No. 03):706–713, 2010.

[12] Prof. A Rama Rao,MKalyani, B Sravanthi, K Pradeep Chandra, and G N Mohan. Performance evaluation of aodv and dsdv routing protocols through clustering in manets. International Journal of Scientific and Engineering