IMPLEMENTATION AND TEST OF A SECURE MECHANISM'S MODULES IN ROUTING PROTOCOL OF MANETS WITH THE THEORY OF GAMES

Dr Karim KONATE and Abdourahime GAYE

Department of Mathematics and Computing, University Cheikh Anta DIOP, Dakar
kkonate911@yahoo.fr
Department of Mathematics and Computing, University Cheikh Anta DIOP, Dakar
agaaye@yahoo.fr

ABSTRACT

The present work is dedicated to the implementation of a secure mechanism's modules in routing protocol of MANET with the theory of games. First we are doing an introduction to what the Mobile Ad hoc Networks (MANETs) and a presentation of some various attacks in MANETs pertaining to fail routing protocols. We study these attacks and the mechanisms which the secured routing protocols use to counter them. In the second hand we also study a reputation mechanism and we also propose a secure algorithm based on the reputation. Our work ends with a proposal analytical model by the theorical games and an implementation to the modules of our mechanism..

KEYWORDS

Mobile Ad Hoc, routing, security, Attacks, reputation, modelling, theory of games

1. INTRODUCTION

For a few years we have assisted an exponential deployment of the spontaneous networks thanks to the emergence of new technologies wireless and of the associated standards, and also thanks to the increasing availability of advanced and autonomous terminals (telephones, PDAs). In the seventies year, the first ad hoc network was born. An Ad hoc network is generally means MANET (Mobile Ad hoc Network) [1].

The MANET is a regrouping of a large population of portable calculating characterized by a dynamic topology, a limited bandwidth, energy constraints, the heterogeneity nodes, and a limited physical security.

Several families routing protocols emerged in MANET. Each protocol can be classified as a reactive like Ad hoc One Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), proactive like Optimized Link State Protocol (OLSR), or hybrid like or Routing Protocol Zones (ZRP) [1].

During the last decade it still problems related security and how to find the investment of lower costs in rated capacities and reserves which ensures the routing of the nominal traffic and guarantees its reliability in the event of any breakdown of arc or node.

2. BACKGROUND

They are many and varied attacks in these MANET:

BlackHole attack: is an attack which the malicious nodes drop some routing messages that they receive. It was declined in several particularity alternatives, having different objectives (Routing loop, Grayhole, Blackmail) [1, 2, 3, 4, 5, 27].

The selfish attack: is an attack which malevolent nodes try to tackle the system: attack on the integrity of the data, the availability of the services, the authenticity of the entities (denial-of-service, interception of messages, usurpation of identity, etc). Selfish nodes are entities economically rational whose objective is to maximize their benefit [8, 9, 10, 28].

Overflow routing tables: consists of malicious nodes to cause the overflow routing tables of nodes being used as relay [4, 20].

Sleep deprivation: consists to make a node to remain in a state of activity and to make him consume all its energy [4, 11, 12, 13, 14].

3. COOPERATIVE MECHANISM

The basic mechanisms of security prove to be effectively ensured the traditional security functionalities which are the confidentiality, the integrity and above all the authentication. They thus ensure to prevent many attacks which disrupt the process of routing. On the other hand, they do not prove to be adapted to resolve the problem of the selfish nodes. Indeed, the cryptographic mechanisms, so effective they are don't ensure a node takes part in the process of routing by relaying all the packets. However, in the context of the ad hoc networks, it's a primordial functionality as far as this type of network is based on the cooperation between the nodes. That's why some protocols aim at more specifically for the incitement to cooperate. Among these solutions, we set those which are based on a reputation nodes elaborated in the course of time according to the observations [1]. Among the protocols which are based on the reputation we can cite CORE which will be the subject of our contribution article.

3.1. The CORE mechanism

The mechanism of CORE [1, 9] encourages the collaboration of other entities by using metric cooperation called reputation and, which is calculated while being based on the local data for each node and can be provided by other nodes of the network implicated in the interchange messages with the supervised nodes. A solution based on punishment mechanism is adopted to prevent a selfish behavior for gradually refusing the communication services to the entities which have bad behavior [1, 9].

3.2. Vulnerabities of CORE

CORE suffers unfortunately from important defects. The mechanism of the reputation is potentially vulnerable face up to the cooperative nodes (BlackHole Cooperative) [1] which agree between them to assign good marks and to allocate in the other hand, bad marks the legitimate nodes. Moreover, in that case the nodes couldn't make the distinction between the useful and the useless messages, and will be obliged to forward all the messages which come through them for having their good reputation. This could generate a waste of energy (sleep deprivation) [11] and moreover the constant monitoring nodes would engender a network overload causing a reduction in the bandwidth. In our algorithm we try to fend off the four vulnerabilities cited for endowing CORE with a mechanism called DRI table [22, 23, 29, 30].

3.3. Operation of DRI table

The DRI or the data table of routing information which is used to identify nodes of cooperative black hole, it consists in adding two additional bits of information. Each node updates an

additional table of information of data routing (DRI) [22, 23, 29, 30]. The following figure represents the structure of the table.

Node #	Data Routing Information	
	From	Through

Figure 1. The structure of the DRI table

In the DRI table, the first bit named "From" represents the information on the packet of the node data routing (the node from which the packets comes) while the second bit "Through" represents the information on the packet by the node of data routing (the node through which its forwards the packets). For example the entry "1,0" for node A means that the node B forwards the packets data coming from A but it doesn't forward any packet of data through A. The entry "1,1" for the node C means that the node B forwards the packets data coming from C and the packets of data through C. This example is represented in table 1.

Table 1. Example of DRI table utilisation

Node #	DRI	
B	From	Through
A	1	0
C	1	1

To discover a route towards the destination node the source node (SN) broadcasts a RREQ message. The intermediate node (IN) which produces a RREP must provide the hop of the next node (NHN) and its DRI entry. According to the RREP message from the intermediate node, the source node will control its own DRI table to see if the intermediate node will a trustworthy node. If the source node used IN before the new route discovery for routing the data, then IN is a reliable node and the source node begins to forward data towards IN. This obliges the attacking nodes to cooperate and to relay messages until the destination to appear in the DRI of its neighbor. This solution can be also adapted to counter the attacks like Overflow, Blackmail and also Selfish.

4. A PROPOSAL SOLUTION AGAINTS THE ATTACKS: COOPERATIVE BLACKHOLE, BLACKMAIL, OVERFLOW, SELFISH

The Reputation and Punishment concepts, or Payment, can encourage the nodes to fully play their role not to lose their good behavior but these solutions cannot counter some attacks in MANETs as the above attacks.

4.1. Description of XCORE

In the existing CORE, we include DRI table and we estimate the table if we receive a routing packet. To making this estimation, we calculate the times that the node has forwarded the

packets coming from another node and the times that the node has forwarded the packets through another node.

If the Rate_Send_Reception rate of the DRI is equal to [0, 0] we declare that this link is fictitious (it's an Overflow attack). Else when a node sends a routing message, we estimate this message. If it's a route error, we will check its validity by looking at the DRI. If Rate_Send_Reception is [0, 0] then we confirm that it's a defective node else we consider that it's an invalid message (if it is a Blackmail attack) and in this case we continue to estimate the reputation. If the reputation is < 0 we consider that it's a denied of service node (a Selfish node) else we declare that it's a cooperating node.

4.2. A proposal mechanism: XCORE

Figure 3 illustrates the operation of XCORE proposed.

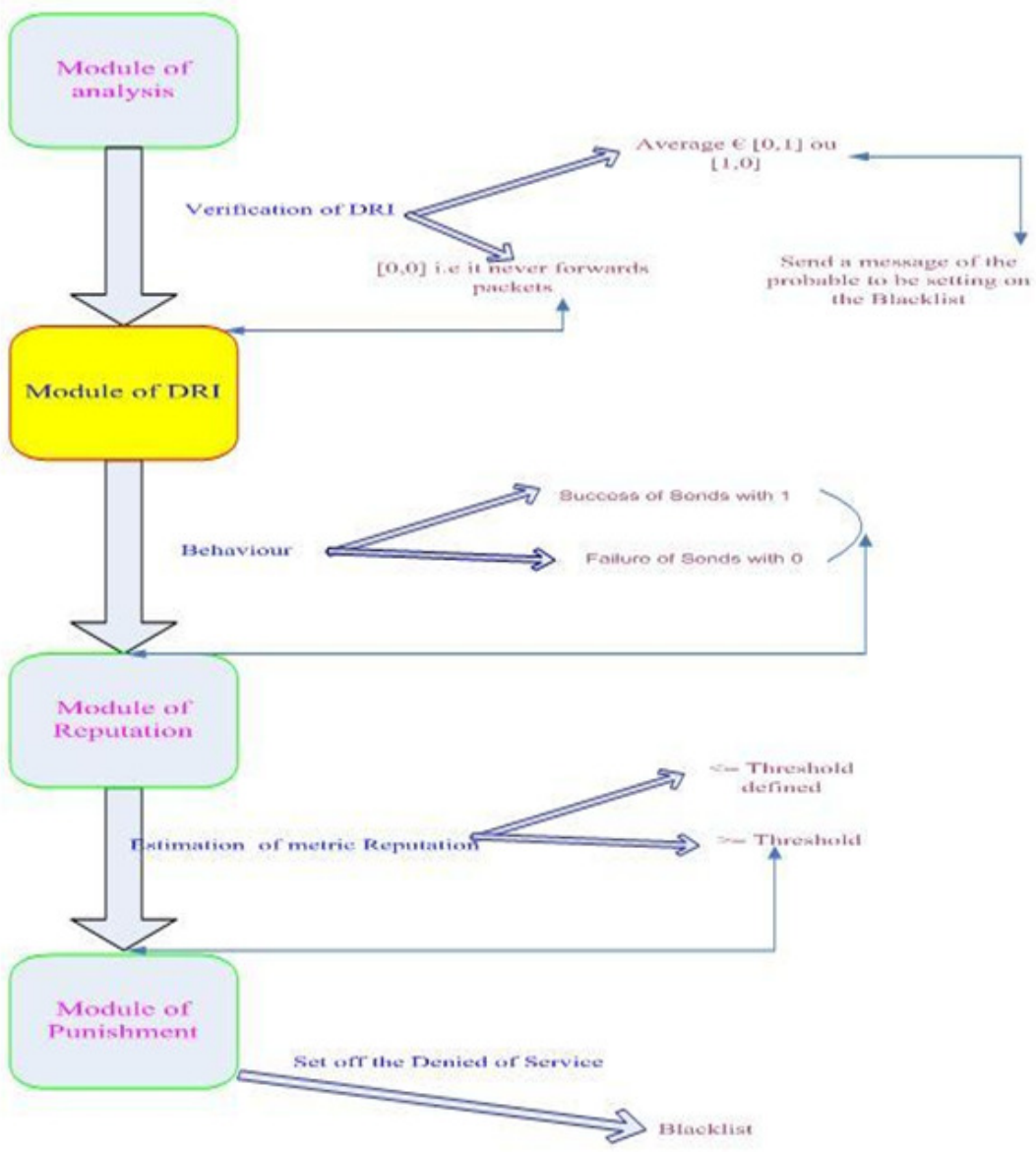

Figure 3. Functioning of XCORE

4.3. Algorithm of XCORE

Begin

- Verification of DRI before transmission;
- If Rate_Send_Reception is equal to [0, 0] then;
- We put the node on the blacklist because it's a fictitious link;
- Else when a node sends a route message, we estimate the message;
- If it's a route error, we will check its validity by looking the DRI;
- If the Rate_Send_Reception is equal to [0, 0] then we confirm that this node is defective;
- Else we consider that this message is invalid (it's a Blackmail attack);
- Else it cooperates for the first iteration and it sends the message by monitoring the node;
- In each iteration of period T, it observes the behaviour of the opposing node and it builds a vector V= (V1, V2, …. VT) which element Vi is shown by 1 for a good behaviour and 0 for a bad behaviour;
- To assess the reputation during this period;
- Reputation= (1/T) * sum of Vi;
- If Reputation >0 then the node is cooperating node;
- Else the node is a denied of service node.

End

4.4. Modelling of our mechanism with the theorical games

To model our proposition we use the prisoner's dilemma (PD) of the game theory [24, 25, 26, 29, 30]. In this traditional model of the PD, two players take with a decision to cooperate (C) or defect (D). If the players cooperate they receive a benefit (G). If the two players decide to defect they receive a punishment (P). In the case or only one player cooperates and the other defect, the benefit will be M for the defected player and N for the cooperated player. The PD is a member of the class named plays with two players, whose sum of the benefits is not null. The dilemma is dictated to the following expressions: $M > G > P > N$, $G > (M+ N) / 2$

The matrix representation is illustrated in the table:

Table 2. The matrix form of PD

Node	Player j		
Player i		C	D
	C	(G, G)	(M, N)
	D	(N, M)	(P, P)

In this section we propose a modelling of some of these attacks like sleep Deprivation and Selfish for using mathematical tools named the game theory which is an analysis's tool of human behaviours. It took an increasing development since the joint publication of Von Neumann and Morgenstern "The Theory of Games and Economic Behavior" in 1944 [24, 25, 26, 29,30]. In [9] the author models the cooperation of the nodes. It is based on the game theory to evaluate the reputation i.e. the behavior of the nodes when they receive messages and transmit them. In the sleep deprivation and Selfish attacks, some nodes receive the messages and decide to process them or not; more they can receive a great quantity of messages coming from an attacking node, thus causing energy consumption. So, we can adapt this approach to model our above mentioned attacks because in this approach the author treats the behavior of the malicious nodes and in the case of our attacks we have to treat the behavior of the malicious nodes.

In the case of our modelling of the attacks sleep deprivation and Selfish, we consider nodes which integrate the network and will decide to communicate. If each of the nodes sends a message and the other decides to process it, each of them consumes energy. On the other hand if the message is not processed (non-cooperation), the sent node loses its energy while the other node saves its energy.

This strategic situation can be described in a more formal way. That is two nodes A and B, each one has two possible strategies (to consume or save) which can be materialized by a function noted $\boldsymbol{\rho}$. With each combination of choice is associated a benefit noted $\boldsymbol{\sigma}$ for node A and the node B. The table gives us examples of benefit in energy. On line we have the choices of node A and in column those of the node B. In each box of table, the first benefit of energy is that of node A and the second benefit is that of the node B.

Table 3. The energy consumption of PD

Nodes	**Node B**		
		Consume	**Save**
Node A	**Consume**	**(- σ , - σ)**	**(- σ , σ)**
	Save	**(σ , - σ)**	**(σ , σ)**

In a general way, if we noted by $\boldsymbol{\sigma}$ the benefit when we execute the function ρ for a reiterated game **k** times for some time **t**;

$$\rho = \begin{cases} Consume, & t = 0 \\ Save \end{cases}$$

If this instant t=1, we apply the cooperation i.e. Consume (sent and processed), the benefit is $U^{t}_{ni}(nj/f)=(-\sigma,-\sigma)$, t=2 we consume $U^{t}_{ni}(nj/f)=((-\sigma,-\sigma),(-\sigma,-\sigma))$, t=3 we consume $U^{t}_{ni}(nj/f)=((-\sigma,-\sigma),(-\sigma,-\sigma),(-\sigma,-\sigma))$ and so on and so forth.

The general formula to calculate the benefit is given by:

$$U^{t}_{ni}(nj/f) = \sum_{k=0}^{t} \rho(k)\sigma k$$

$U^{t}_{ni}(nj/f)$ is the benefit got in time t by the node ni on the node nj for executing the function f

$\rho(k)$ is a function which depends on time recording the values of σk

σk represents the benefit obtained with the kth iteration when we execute the action $\rho(k)$.

For example, if node A sends and B doesn't process, A consumes -2 Joules and B saves 2 Joules and vice versa. If node A sends and B processes, each of them consumes -2 Joules. If the nodes do not send nor process, they will save 2 Joules. The following Table gives us an example of energy consumption for the nodes which are communicated.

Table 4. An example of PD energy consumption

Nodes	Node B		
Node A		Consume	Save
	Consume	(-2, -2)	(-2, 2)
	Save	(2, -2)	(2, 2)

For the modelling of DRI module, always we consider the example of nodes A and B. That is two nodes A and B, each one has two possible strategies (forward or never forward). We have the following table which represents the matrix of DRI.

Table 5. The matrix of DRI

Nodes	Player j		
Player i		Forward	Never Forward
	Forward	(G, G)	(M, N)
	Never Forward	(N, M)	(P, P)

For example, if the nodes A and B forward the packets of the one through the other, each one benefits an entry equal to 1 for its DRI table, if node A forwards the packets through B and B has never forwarded through A, A benefits an entry equal to 1, B benefits 0 and vice versa. If

the nodes have never forwarded the packets of the one of the other, they perceive an entry equal to 0.

Table 6. An example of DRI matrix

Nodes	Node B		
Node A		Forward	Never Forward
	Forward	(1, 1)	(1, 0)
	Never Forward	(0, 1)	(0, 0)

5. IMPLEMENTATION AND TEST OF MODULES WITH THE GAME THEORY

5.1. The test of the prisoner's Dilemma (DP) associated with the energy consumption

To test our game theory, we consider a scenario where the nodes decide to send messages or not. We give in entry the number of nodes (N), Nc which corresponds to the number of cooperate nodes and Na the number of selfish nodes. The play is repeated Nb times and means the number of observations in time. On each sent or received packet, the consumption energy is equal to a variable noted Ce. The evaluation parameters are represented in table 7.

Table 7. The test parameters of the prisoner's dilemma (DP)

Parameters in entry	Values
Number of de nodes (N)	50
Number of cooperate Nodes	Nc
Number of selfish Nodes	Ne
Number of observations (Nb)	[1,50]
Consumption energy of cooperation (Ce) in J	0 ,3

The following figure illustrate the energy conservation

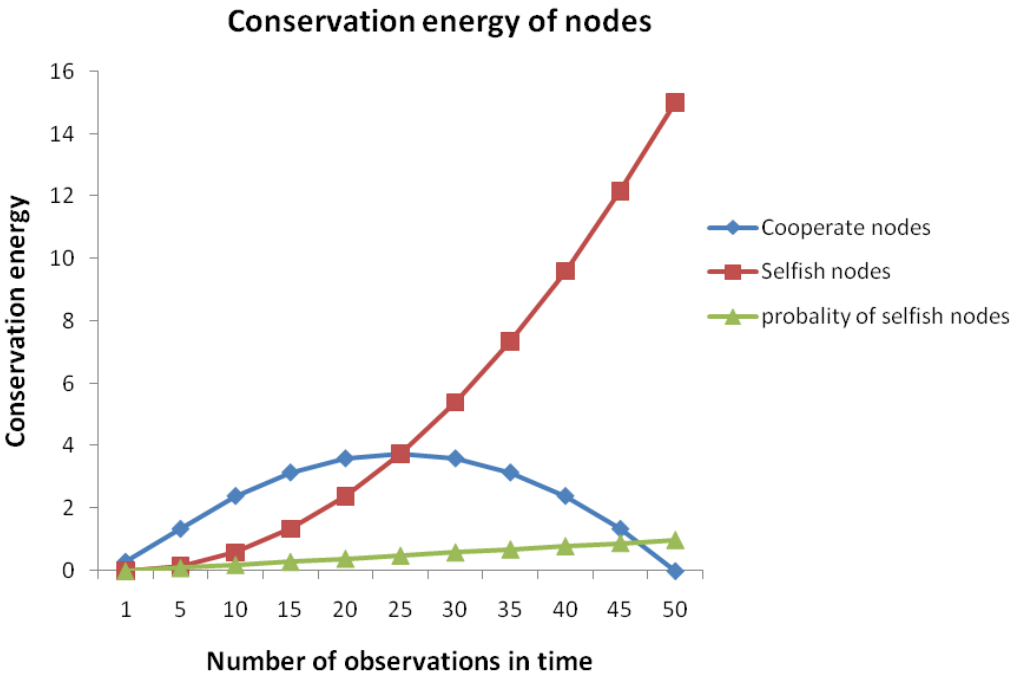

Figure 4. Energy conservation with the DP

For an iteration count equal to 1, we note that the energy consumption is equal to 0. That can be explained owing to the fact that all the nodes of the network take part in the smooth functioning for not consider them to be selfish in order to be isolated thus no possibility of energy conservation.

When the number of observations is equal to 25 the energy conservation of the cooperating nodes reaches its maximum (approximately 4 J) and starts to decrease up to 0 if this number is equal to 50 while the energy conservation of the selfish nodes is an ever increasing and reaches a value equal to 16 J.

Thus we note an increase in the energy conservation of the selfish nodes and a reduction in that of the cooperating nodes when the play is repeated in time. That finds its explanation as the model of the DP shows it by the fact that if the nodes decide to cooperate, they will lose their energy out of which the nodes tend to be selfish in order to remain longer in the network and to play fully their part.

5.2. The test of the DRI module

To test our module DRI, we gave in entry the DRI iteration count, the From value means that node in the network has routed a packet coming from a node and the Through value means that node in the network has routed a packet through a neighboring node. If the Aver_from_through average of the DRI belongs to [0.0] we declare that this link is fictitious (it's an Overflow attack). If not when a mobile sends a route message, we evaluate this message. If it is a route error, we will check his validity by looking at the DRI. If Aver_from_through is [0.0] then we confirm that this node is defective else we consider that this message is not valid (it's a Blackmail attack). The evaluation parameters are represented in table 8.

Table 8. The test parameters of the DRI module

Parameters in entry	Values
Number of observations	[1,50]
From	[0,1]
Through	[0,1]

The following figure illustrate the functioning of DRI module

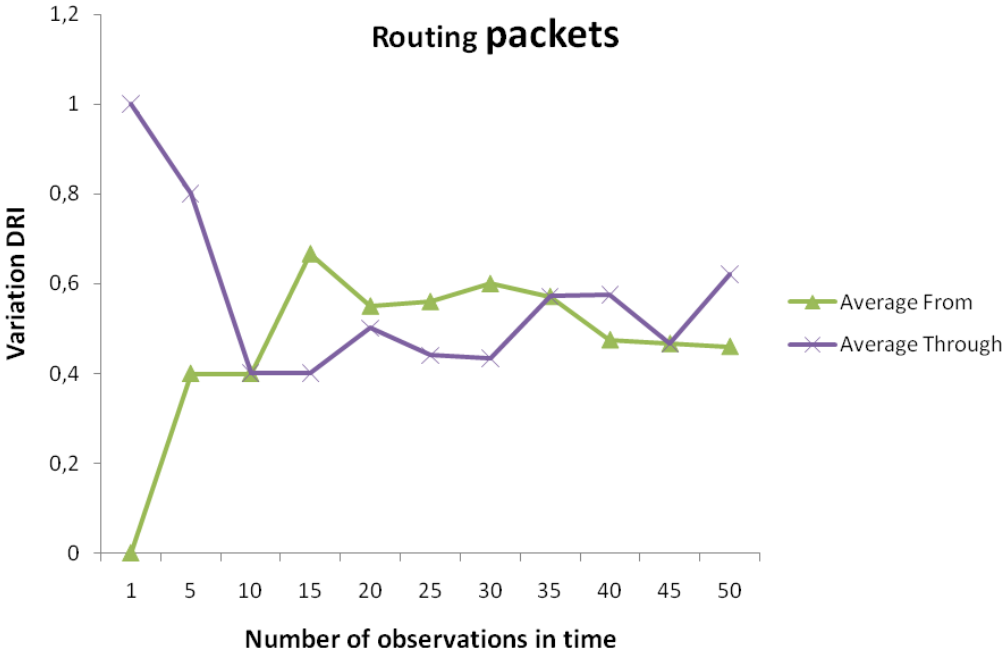

Figure 5. Functioning of DRI module

For a number of observations equal to 1, we have an Aver_from_through average of the DRI belongs to [1,0]. That means that node has routed the packets coming through its neighbor but doesn't route packet through this last. This average enables us to check the validity of the maintenance messages like the route error sent by nodes of the network and also the declarations of fictitious nodes.

From a number of observations equal 5, Aver_from_through of the DRI belongs to]0,0[and almost keeps the same value up to 50 observations. Thus we note a fall of DRI average when the number of observations increases. That finds its explanation by the fact that the nodes will not spend their time to send or receive packets, which makes it possible to fight against the sleep deprivation.

Thus on the one hand, to detect the cooperative BlackHole attack the evaluation of the validity of the messages is necessary before isolating a node in the network. On the other hand, so that a node is considered as selfish or not we are obliged to evaluate his reputation in order to determine the failure or the success rate associated with this node.

5.3. The test of the Reputation module

To test the module of reputation, we consider a scenario which evaluates the success or the failure of sending messages. We give in entry the indices of reputation (0 mean failure and 1 means successes), Nc corresponds to the number of nodes which undertook to cooperate and Na the number of selfish nodes. The evaluation of the reputation will be carried out on Nb observations in time. If the reputation is ≤ 0 we consider that this node is a denial of service node (a Selfish node) else we declare that this node is a cooperating node. In TRP this rate is replaced by the confidence indexes and in this case we consider only the second value of rate but also the checking of the route error messages is necessary. The evaluation parameters are represented in table 9.

Table 9. The test parameters of the Reputation module

Parameters in entry	Values
Index of reputation	[0,1]
Period of reputation evaluation (Nb)	[1,50]
Value of the reputation	$\leq 0, \succ 0$

The following figure illustrate the functioning of Reputation module

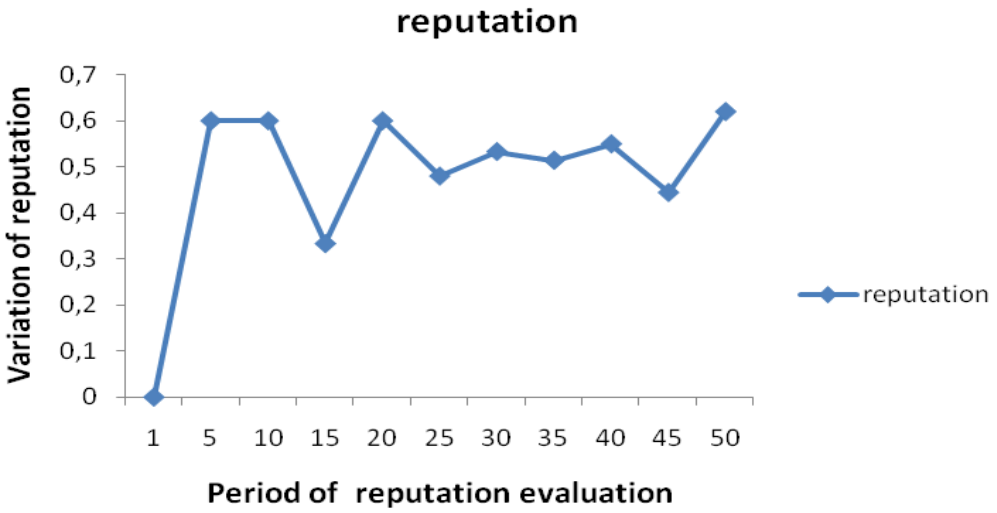

Figure 6. Functioning of Reputation module

For one period of reputation evaluation equal to 1, we have 0 like reputation value. That means that node is considered by its neighbor as a denial of service node. When the period of evaluation is equal to 5, the reputation is > 0 and knew a fall when the value is equal to 15 before starting to rectify up to one period of evaluation equal to 50.

Thus we note a variation of the reputation when the evaluation period increases in time. That finds its explanation by the fact that the nodes which are in the network with the time will detect the selfish nodes, which enables them to gain confidence in order to be considered as cooperating nodes.

6. RESULTATS AND DISCUSSION

Cooperation is intended as the willingness of a node to perform networking functions for the benefit of others nodes. However, cooperation has a non-negligible energetic cost that can lead to a selfish behavior, especially in battery powered environment such as mobile ad hoc networks.

Thus to support the cooperation of the nodes, our model suggests to use the DRI table to detect the declaration of fictitious nodes (Overflow attack) just as the sending of false messages which announce a malicious node whereas last is legitimate causing an attack blackmail like illustrating in the tables below. The nodes can be satisfied with these contained informations in these tables to see whether the node is legitimate or not, which makes it possible to encourage the cooperation (against the selfish) and also to be able to save energy in the event of presence of the virtual nodes (against the sleep deprivation).

We have implemented all the modules of our mechanism in order to make real test and to see the impact of these modules. It would be interesting to see the stability of the nodes by using the balance's Nash of the theorical games

7. CONCLUSIONS

Mobile ad-hoc routing and forwarding are vulnerable to misbehavior, which can occur due to selfish, malicious, or faulty nodes. Solutions to the problem of misbehavior have so far been classifiable into three main categories: payment systems, secure routing, and detection and reputation systems. Payment systems target selfish misbehavior by providing economic incentives for cooperation. Secure routing proposals aim at the prevention of malicious misbehavior. Self-policing systems that consist of detection, reputation, and response components target at the isolation of misbehaved nodes regardless of the reason for misbehavior. None of these solution approaches alone can do prevention, detection, and response.

In our work we have presented the specificities of the MANET as well as the problems of the security routing protocols in these types of network. We presented some attacks met in MANETs, their functioning mode thus the mechanisms used and the protocols which implement them to counter these attacks.

We analyzed the functioning mode of CORE and brought out some of its vulnerabilities, and then we proposed a new algorithm, named XCORE, which improves the basic CORE. This algorithm ensures to resist the attacks BlackHole cooperative, Blackmail, Overflow, and Selfish. We modelled the modules of XCORE by using the theory game to see the impact of selfish and the energy consumption. We have implemented the modules of the mechanism in C++ to see the variation. In the future we propose to implement the XCORE in order to make evaluations of performance with CORE.

REFERENCES

[1] Wiley John: Security for Wireless ad hoc networks. Eyrolles, book 2007, pages 247.

[2] Adjido Idjiwa,Benamara Radhouane,Benzimra Rebecca,Giraud Laurent: Protocol of secure routing ad hoc in a clusterized architecture. University Pierre and Marie Curia(Paris VI), FRANCE, November 2005, pages 4.

[3] Curtmola Reza. Security of Routing Protocols in MANET. 600.647-Advanced Topics in Wireless Networks,February 2007, pages 26.

[4] Bing Wu,Jianmin Chen,Jie Wu,Mihaela Cardei. A Survey of Attacks and Countermeasures in MANET. Department of Computer Science and Engineering Florida Atlantic University, Decembre 2005

[5] Chen Ruiliang,Snow Michael,Park Jung-Min,M. Refaei Tamer,Eltoweissy Mohamed. Defense against Routing Disruption Denial-of-Service Attacks in MANET. Department of Electrical and Computer Engineering Virginia Polytechnic Institute and State University Blacksburg, VA, USA, November 2005, pages 15.

[6] A.Rajaram,Dr. S. Palaniswami. The Trust-Based MAC-Layer Security Protocol for Mobile Ad hoc Networks.(IJCSE) International Journal on Computer Science and Engineering Vol.02 ,No.02, 2010, 400-408. Anna University Coimbatore, India, March 2010, pages 9.

[7] T.V.P.Sundararajan et Dr.A.Shanmugam. Behavior Based Anomaly Detection Technique to Mitigate the Routing Misbehavior in MANET. Sathyamangalm-638401,Tamilnadu, India, May 2009, pages 14.

[8] Kevin Hoffman,David Zage,and Cristina Nita-Rotaru. A Survey of Attack and Defense Techniques for Reputation Systems. Department of Computer Science and CERIAS Purdue University. April 2008, pages 19.

[9] Pietro Michiardi: Cooperation in the ad hoc networks: Application of the evolution and game theory within the framework of imperfect observability. Institute Eurecom 2229, road of the Peaks LP 19306904 Sophia-Antipolis, France, July 2006 ,pages 17.

[10] Michiardi Pietro and Molva Refik: CORE: A Collaborative Reputation Mechanism to enforce node cooperation in MANET. European Wireless Conference, November 2003, pages 15.

[11] Hu Jiangyi: Cooperation in Mobile Ad Hoc Networks. Computer Science Department Florida State University, January 11 2005, pages 23.

[12] Buttyan Levente and Hubaux Jean-Pierre: Nuglets: a virtual Currency to Stimule Cooperation in Self-Organized Mobile Ad Hoc Networks. Institute for Computer Communications and Applications Department of Communication Systems Swiss Federal Institute of Technology Lausanne, 18 January 2001, pages 15.

[13] Yan Zheng, Zhang Peng,Virtanen Teemupekka. Trust Evaluation Based Security Solution in Ad Hoc Networks. Helsinki University of Technology,Finland, December 2003, pages 14.

[14] Xue Xiaoyun. Security mechanisms for ad hoc routing protocols. Computer Science and Network Department,ENST, thesis September 2006, pages 234.

[15] Pietro Michiardi and Refik Molva. Analysis of Coalition Formation and Cooperation Strategies in MANET. Institut Eurecom May 2004, pages 28.

[16] Levente Buttyan and Jean-Pierre Hubaux. Report on a Working Session on Security in Wireless Ad Hoc Networks. Laboratory for Computer Communications and Applications Swiss Federal Institute of Technology-Lausanne(EPFL), Switzerland,September 2002, pages 17.

[17] Pietro Michiardi - Refik Molva. Game theoretic analysis of security in mobile ad hoc networks. Institut Eurécom Research Report N°RR-02-070, juin 2002, pages 10.

[18] Hu Yih-Chun,Perrig Adrian,Johnson David B.: Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, INFOCOM 2003, pages 11.

[19] Emmanouil A. Panaousis, Levon Nazaryan, Christos Politis. Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications,Wireless Multimedia and Networking(WMN) Research Group Kingston University London. July 2009, pages 7.

[20] Shang-Ming Jen 1,Chi-Sung Laih 1 and Wen-Chung Kuo. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET.

[21] Payal N. Raj,Prashant B. Swadas. DPRAODV: A Dynamic Learning System Against Blackhole Attack In Aodv Based Manet,IJCSI International Journal of Computer Science Issues, Vol.2, Computer Engineering Department,SVMIT Bharuch, Gujarat,India, September 2009, pages 6.

[22] Ramaswamy Sanjay,Fu Huirong,Sreekantaradhya Manohar,Dixon John and Nygard Kendall: Prevention of Cooperative BlackHole Attack in MANET. Department of Computer Science, IACC 258 North Dakota State University, Fargo,ND 58105, March 2003, pages 7.

[23] Hesiri Weerasinghe and Huirong Fu. Preventing Cooperative BlackHole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation;International Journal of Software Engineering and Its Application Vol.2 ,No.3. Oakland University Rochester MI 48309 USA, June 2008, page 16.

[24] Caruso Xavier.Théorie des jeux. Librement inspiré du cours d'Ivar Ekeland , Avril 2004, pages 8.

[25] Penard Thierry. La Théorie des jeux et les outils d'analyse des comportements Stratégiques. Université de RENNE 1, CREM; octobre 2004, pages 38.

[26] Thisse Jacques François. Theorie des jeux : une introduction. Recherches Economiques de Louvain, vol. 36, 21-37, 1970 ; octobre 2003, pages 62.

[27] E.Venkat Reddy. Trustworthy Robust Routing Protocol for Mobile Ad Hoc Network, International Journal of Engineering Science and Technology Vol.2 (2), 2010, 77-86, Amina Institute of Technology, Hyderabad, Andhra Pradesh-India, Fevrier 2010, pages 10

[28] Chanet Jean-Pierre : Algorithme de routage coopératif à qualité de service pour des réseaux ad hoc agri-environnementaux. No d'Ordre : 1745 EDSPIC : 373, Université Blaise Pascal - Clermont II, Janvier 2009.

[29] Dr K KONATE, A GAYE: Analysis of Attacks in mobile ad hoc networks: Modeling and Simulation. 2nd International Conference on Intelligence Systems, Modeling and Simulation (**ISMS2011**), **ISBN 978-0-7695-4262-1** Kuala Lumpur (Malaysia) January 2011.

[30] Dr K KONATE, A GAYE: A mechanism against the attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in mobile ad hoc networks. The 2010 International Conference on Future Generation Communication and Networking, Jeju Island, Korea, December 2010, ISSN: ISSN: 2233-7857, Vol 4, num 2.

Authors

Abdourahime GAYE
Student Researcher Department of Mathematics and Computing University Cheikh Anta DIOP, Dakar