MODELLING OF A SECURE MECHANISM IN ROUTING PROTOCOL OF MANETS: APPLICATION OF 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 study of attacks and countermeasures in MANET. After a short introduction to what the Mobile Ad hoc Networks (MANETs) are and network security we present a survey of various attacks in MANETs pertaining to fail routing protocols. We present the different tools used by these attacks and the mechanisms used by the secured routing protocols to counter them. We also study a mechanism of security, named the reputation, proposed for the MANETs and the protocol which implements it. We also propose a secure mechanism which is based on the reputation. Our work ends with a proposal analytical model 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].

An Ad hoc network constitutes a regrouping of a large population of portable calculating units (laptops, telephones…) inter-connected by a wireless technology, moving in an unspecified territory, forming a decentralized network, without fixed infrastructure.

In mobile ad-hoc networks, nodes act as both routers and terminals. For the lack of routing infrastructure, they have to cooperate to communicate. Cooperation at the network layer takes place at the level of routing, i.e. finding a path for a packet, and forwarding, i.e. relaying packets for other nodes. Misbehavior means aberration from regular routing and forwarding behavior resulting in detrimental effects on the network performance. Misbehavior arises for several reasons. When a node is faulty its erratic behavior can deviate from the protocol and thus produce non intentional misbehavior. Intentional misbehavior aims at providing an advantage for the misbehaved node. An example for an advantage gained by misbehavior is power saved when a selfish node does not forward packets for other nodes. An advantage for a malicious node arises when misbehavior enables it to mount an attack.

This network is usually characterized by a dynamic topology, a limited bandwidth, energy constraints, the heterogeneity nodes, and a limited physical security. The applications having recourse to the ad hoc networks cover a very broad spectrum. For example in the tactical applications (fires, flood, etc.), in the soldier's field, in the monitoring systems, and the world of transport [1].

DOI : 10.5121/ijdps.2011.2628

The problem of the MANET is 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. That's why several families routing protocols emerged. 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].

In spite of the evolution ad hoc mobile networks during the last decade it still problems related security which remain unsolved. Although some solutions were proposed none of them can't satisfy all the constraints on the ad hoc networks.

2. BACKGROUND

An attack is an action which aims at compromising the security of the network. They are many and varied in these MANET:

BlackHole attack: consists in dropping some routing messages that node receives [1, 2, 3, 4, 5, 27]. It was declined in several particularity alternatives, having different objectives, among which we can quote:

- Routing loop, which makes it possible for a node to create loops in the network;
- Grayhole, which lets pass only the packages of routing and diverts the data;
- Blackmail, which makes it possible for a node attacker to isolate another node.

Several solutions exist to counter these types of attacks, among which we name the technical estimate relation. In this mechanism the authors classified the relation between the nodes and their neighbors in three cases: Unknown (node X sent forever (received) of messages to (from) the node y and the probability of the malevolent behaviour are very high), acquaintance (node X sent (received) some messages to (from) the node y and the probability of the malevolent behavior must be observed) and Friend (node X sent (received) in abundance of the messages to (from) the node y and the probability of the malevolent behaviour is too small. This mechanism is implemented in the routing protocol RDSR (Relationship enhanced DSR protocol) [6].

The Threshold of sequence number consists in performing a check to find if RREP_seq_no is higher than the threshold value. The threshold value is dynamically updated in each interval of time. As the value of RREP_seq_no proves higher than the threshold value, one suspects the node to be malicious and adds it to the black list. This mechanism is implemented in the routing protocol named Detection, Prevention and Reactive AODV (DPRAODV) [21].

The Watchdog or monitoring (watchdog) is a solution which makes it possible to identify malicious nodes. The Watchdog assigns positive values with a node which successfully forwarded packages and a negative value after a threshold level of bad behavior was observed. It's implemented in the protocol called mobile Secure Watchdog for Ad hoc Network (SWAN) [14]. Pathrater which makes it possible the protocol to avoid nodes corrupted register in a black list [14]. The DRI or the data table of information's routing which is used to identify nodes of cooperative BlackHole, it consists in adding two additional bits of information. These bits have as values 0 for "FALSE" and 1 for " TRUE " for intermediate nodes answering the RREQ of node source; AODV implements this mechanism [22, 23]. The Cross checking solution which consists in hoping on reliable node (nodes by which node source has forwarded the data) to transfer from the packets of data [22, 23].

The selfish attack: consists in not collaborating for the good performance of the network. We can identify two types of nodes which do not wish to take part in the network. Defective nodes i.e. do not work perfectly. Those which are malevolent, it is those which intentionally, 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. To prevent the selfish nodes some solutions were proposed. Among these we have a solution based on the Negative Selection Algorithm (NSA). It's based on the principles of the discrimination of self or no self in the immune system (to define it to oneself like a collection S of elements in a characteristic space X, a collection which needs to be supervised) [21]. The detection of anomaly aims at distinguishing a new model like part of self or no-self, given a model of system of self [21]. Structured Gene Activation (SGA) is a type of evolutionary algorithm which incorporates the redundant genetic material, which is controlled by a mechanism of . It uses the multi-layer genomic structures for its chromosome i.e. all the genetic material (expressed or not) "is structured" in a hierarchical chromosome. The activation and deactivates mechanism these coded genes. This solution is implemented in AODV [21]. A solution based on the reputation named Collaborative Reputation (CORE) and Cooperation of Nodes and Fairness in Dynamic Ad-hoc Network (CONFIDANT) which consists in collecting information on an old behaviour of the tested entity by others [8, 9, 10, 28]. A solution based on the payment (Nuglet) which requires with nodes which benefit from the resources of the network (transmitters and/or receivers) to pay "service providers" (intermediate nodes) [9, 10, 28] and a solution based on the localization (directional antennas).

Overflow routing tables: consists of malicious nodes to cause the overflow routing tables of nodes being used as relay [4]. To fend off this attack the named solution Trust evaluation was proposed. It's based on the evaluation of confidence to ensure a secure routing in MANETs. The success of a communication through a node will increase the index of confidence of this node and the failure by this node will decrease the index of confidence. If this value reaches zero this node is registered in a blacklist and we inform the other neighbors. Trust-based Routing Protocol (TRP) implements this solution [20].

Sleep deprivation: consists to make a node to remain in a state of activity and to make him consume all its energy [4]. To fend off the sleep deprivation we have recourse to some solutions. One which is based on the selection of advised energy and which takes into account the energetic considerations in the choice of the best route. Each node calculates its own energetic statute and declares an appropriate prediction. The choice of the prediction is based over the capacity of the battery and the lifetime envisaged of a node. The relationship between real and initial energy of a node is used to measure the capacity of battery. This mechanism is implemented in protocol EEAOMDV: Energy Efficient Ad hoc One Demand Multipath Outdistances Vector Routing Protocol [11]. One which is based on the effective Energy for the routing; it requires a dynamic commutation on the states of the nodes between the sleep mode and the active mode. The nodes enter these states with fixed intervals in order to ensure the forwarding of the messages successfully; the active nodes can retransmit messages some times before the node of destination is in listening or activity. This mechanism is implemented in BECA: BASIC Energy Conserving Algorithm [12]. One which is based on PARO (control of power of the routing) which is a technique of control power routing for MANETs where all nodes are located in the maximum range transmission of the one another i.e. energy depends on the distance which separates the source and the destination [13]. The solution which is based on PAA (Alternation of the control power) consists in eliminating the network activity for a group of nodes during some period in order to preserve their energy and to keep their presence in the network by a delegation [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] is used to impose the cooperation of the nodes. In CORE each entity of the network encourages the collaboration of other entities by using metric cooperation called reputation. This metric is calculated while being based on the local data for each node and can be based optionally on the information provided by other nodes of the network implicated in the interchange messages with the supervised nodes. This reputation is based on the analysis of the behavior (Watchdog) associated each node. A Boolean vector represents a good (with one 1) or a bad (with one 0) behavior. A punishment mechanism is adopted as solution to prevent a selfish behavior for gradually refusing the communication services to the entities which have bad behavior. This punishment is applied if the metric of reputation (Pathrater) reached a threshold and in this case we declare that the selfish nodes constitute a denial of service and they will be put in the blacklist. Thus the legitimate nodes (which cooperate) reach to save energy.

3.2. Vulnerabities of CORE

CORE suffers unfortunately from important defects. First, it doesn't really resolve the problem of selfish [1]. Immediately, all the selfish nodes see their packets rejected systematically and in this, the protocol is effective. But on the other hand, a quantity of data remains lost, reducing significantly the efficiency of the network. The protocol is based on assumptions (secure routing, single and nonusurpable addresses) which still remain to make a reality. It's a common disadvantage to all the reputation protocols. Indeed, this one is based on the information observed for the nodes and consequently requires an authentication mechanism in order to affect the marks to the legitimate which could store nonexistent links thus causing the Overflow attack [01]. In addition, it's difficult to avoid the problem of fictitious denunciation (Blackmail) [1] in which a malicious node generates false messages to put up the legitimate nodes on the blacklist. 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].

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. These bits have as values 0 for "FALSE" and 1 for " TRUE "for intermediate nodes answering the RREQ of node source. Each node updates an additional table of information of data routing (DRI) [22, 23]. 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.

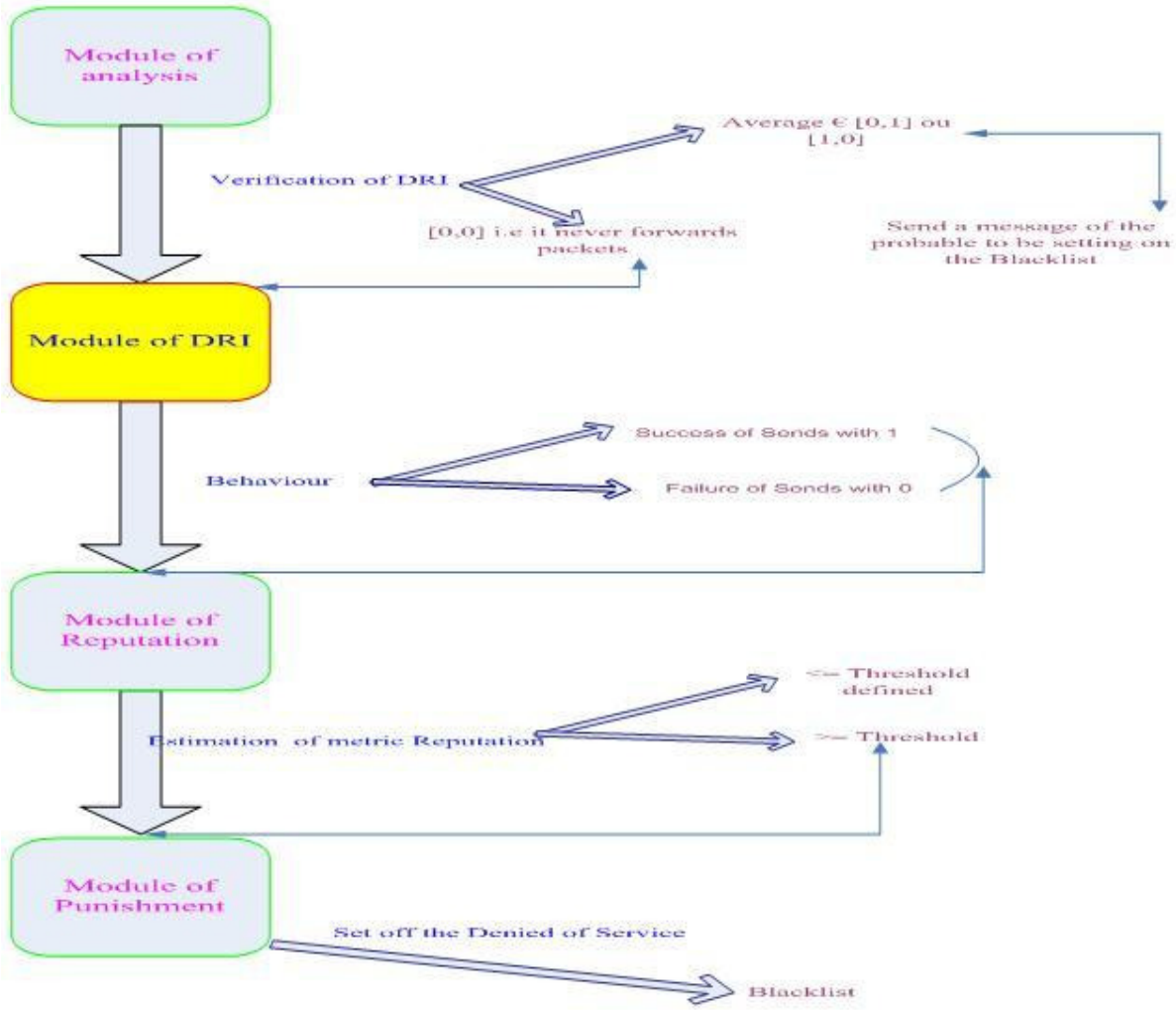

Figure 3. Functioning of XCORE

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 $\succ 0$ 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]. 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]. 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 ρ. With each combination of choice is associated a benefit noted σ 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	$(-\sigma, -\sigma)$	$(-\sigma, \sigma)$
	Save	$(\sigma, -\sigma)$	(σ, σ)

In a general way, if we noted by σ 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:

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

$\mathbf{U^{t}_{ni}(nj/f)}$ 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. 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). In the future we propose to implement all the modules of our mechanism in order to make real test because in this work we presented only theorical test.

6. 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. 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.

Authors

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