A GAME THEORETIC APPROACH TO GRAY HOLE ATTACKS IN WIRELESS MESH NETWORKS

Devu Manikantan Shila, Tricha Anjali
Department of Electrical and Computer Engineering
Illinois Institute of Technology
Chicago, IL 60616
Email: {dmanikan, anjali}@iit.edu

I. ABSTRACT

Wireless Mesh Networks (WMNs) are multi hop networks in which the mesh clients rely on static mesh routers (or directly via other mesh clients) to relay data from one point to another in a multihop fashion. WMN gained significant attention because of the numerous applications it supports, e.g., broadband home networking, community and neighborhood networks, delivering video, building automation, in entertainment and sporting venues etc. But the main challenge of these multihop networks is the susceptibility to various security threats. In this paper, we address the problem of gray hole attack in which a malicious node refuses to forward a subset of the packets it receives. We present the attack in a simple network of mesh routers in the framework of a non-cooperative markov game between genuine and malicious mesh router. The main objective of the legitimate node ($Player\ I$) is to maximize its throughput by minimizing the loss caused by the attackers. On the other hand , the main goal of the attacker ($Player\ II$) is to minimize the throughput of the network by dropping the data packets. We investigate the nash equilibrium of the non cooperative game by allowing the nodes to select their own actions that optimizes the individual performance in terms of the packet delivery ratio.

II. INTRODUCTION

Using Wireless Mesh Networks (WMNs) [1] to provide better wireless services in the future is emerging as a popular choice for Internet Service Providers (ISPs) because of the advantages like reliability, market coverage, scalability and low upfront cost. WMNs also play a significant role in broadband home networking, community and neighborhood networks, delivering video, building automation etc. However, WMNs lack security guarantees in various protocol layers and hence it is not yet ready for wide-scale deployment. The main reasons for the security challenges are due to the open medium, dynamic topology, and distributed architecture of the mesh networks [1], [2].

In a WMN, there are two types of nodes: mesh routers and mesh clients. Mesh routers are static and they form the backbone of the network. Mesh clients can access the network through these mesh routers in a multihop fashion. It is not difficult to understand that routing plays a significant role in a multihop communication and hence the focus of most of the malicious attacks like gray hole attacks, sybil attacks, denial of service attacks etc. In this work, we focus on the gray hole attacks (aka selective forwarding attacks)[3], [4]. Section III discusses the gray hole attacks and the related works in this area in detail.

Game theory has been used extensively to model the wireless networks because of its ability to analyze the interaction between a group of nodes (or players) who behave strategically [6], [7]. Some of the earlier works [8], [9] used a game theoretic approach to model Intrusion Detection in wireless networks. In this paper, we consider a simple network of mesh routers, with a source node, destination node and an intermediate node. The source node can use direct path to communicate with destination or rely on an intermediate node to transmit packets to the destination. In most of the previous works [10], [11], we can see that the authors' focus on increasing the cooperation between the source node and the intermediate node by using a reward based mechanism so that the source node can use minimum energy path for transmission. But, we believe that the source node should also take into consideration the reliability of the path. In this paper, we formulate the forwarding problem (direct transmission or routed transmission) as a non cooperative two player markov game from the perspective of security and show the relevance of security in selecting paths.

Throughout the paper, we will interchangeably use the terms players and nodes to denote the mesh routers in the network. The rest of the paper is organized as follows: Section III presents an overview of the gray

hole/selective forwarding attacks against the mesh network. In section IV, we introduce to the readers the basic concepts of game theory and the general model of the stochastic game. Section V discusses the game model, rewards and costs for the strategies of the players, the transition rule and the expected utilities for each player. In section VI, we present the numerical analysis and the results of the game model. Finally, we conclude this paper and discuss our future work in Section VII.

III. Gray Hole/Selective Forwarding Attacks

In a gray hole attack [3], [4], [5], a malicious node refuses to forward certain packets and simply drops them. If a malicious node drops all the packets, the attack is then called a black hole which is easy to detect as opposed to a gray hole attack in which the attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. To launch this kind of attack, an attacker may compromise or hijack the physically unprotected mesh routers that belong to the network (known as internal attacks) or attack the network from outside by jamming the communication link between the routers (known as external attacks). In this paper, we consider these attacks and formulate a game in which the sender ($Player\ I$) selects a strategy that minimizes the loss caused by this kind of attacker ($Player\ II$).

Karlof $et\ al.$ [3] first discussed the selective forwarding attacks and suggested that multi path forwarding can be used to counter selective forwarding attacks in the area of sensor networks. But the main disadvantages of multi path forwarding are overhead, poor security resilence etc. In [4], the authors presented a multi hop acknowledgement scheme for detecting gray hole attacks. In their scheme, the intermediate nodes are responsible for detecting the misbehavior of the nodes. If a misbehavior is detected, it will generate an alarm packet and deliver to source node. The two main disadvantages of this scheme are (a) The intermediate nodes in the path suffer from high overhead. (b) The scheme will not work if a node is compromised during the deployment phase by the attacker.

In [5], the authors present a Counter-Threshold based detection algorithm to defend these attacks. The algorithm uses the path throughput and packet counter to identify the attacks. If an attacker is detected, the algorithm invokes the second phase of the algorithm called Query-Based. This phase uses acknowledgment from the intermediate nodes to localize the attacker.

IV. Game Theory

Game theory [7] can be defined as the mathematical model to analyze the interaction between a group of players who behave strategically. The ability to model individual, independent players whose strategies affect every other players in the group makes game theory a powerful and useful tool to analyze the performance of wireless mesh networks. In other words, game theory is concerned with finding the best strategies for individual players in such dynamic, distributed and unpredictable wireless networks [8]. A game is usually specified by four objects:

- A set of players $i \in N$, which is a finite set $\{1, 2, 3, ...n\}$.
- The strategy space, A_i, available to each player i. When a player chooses an action, he can use either a pure or a mixed strategy. If the actions of the player are deterministic, he is said to use a pure strategy. A mixed strategy is a probability distribution over a player's pure strategies.
- The payoffs, u_i, associated with any strategy combination (one strategy per player).
- All players are rational and each player chooses action that yields him the greater payoff. If the game is not deterministic, the players chooses action that maximize his expected payoff.

We will now discuss some of the important terms in game theory which will be used in this paper.

1) Non-Cooperative and Cooperative Game: In non-cooperative games, the actions of the single players are considered and in cooperative games the joint actions of the players are considered.

2) Complete and Incomplete Information Game: Non-cooperative games can be classified as complete information games or incomplete information games, based on whether the players have complete or incomplete information about their opponents in the game. In games with complete information the preferences of the players are common knowledge, that is all the players know all the utility functions. But in a game of incomplete information the players do not know some relevant characteristics of their opponents which include their payoffs, strategy spaces etc.

3) Zero-sum and Non Zero-sum Game: In a (two player) zero-sum game, the payoffs of the player I are just the negative of the payoffs of player II; that is $u_1(s_1, s_2) + u_2(s_1, s_2) = 0$. If the sum of the payoffs is not equal to zero, $u_1(s_1, s_2) + u_2(s_1, s_2) \neq 0$, then it is a non-zero sum game.

4) Definition of Stochastic Games: A markov game, also called a stochastic game [6] is defined by a set of state variables $k \in K$, a collection of action sets, $A_1, A_2, ...A_i$, one for each player i, $Q : K \times A_1 \times ..... \times A_i \rightarrow PD(K)$ is a transition probability function and $U_i : K \times A_1 \times .... \times A_i \rightarrow \Re$ is an immediate utility function for player i. Assume that the game is in state $k^t \in K$ in time t and players select the actions $a_1^t \in A_1 \cdots a_i^t \in A_i$. Each player i will receive an immediate utility or reward of $U_i(k^t, a_1^t \cdots a_i^t)$ and the game will move to next periods state $k^{t+1} \in K$ with probability given by the transition function $Q(k^{t+1}/k^t, a_1^t \cdots a_i^t)$. The readers who are interested in game theory can refer the following references [6], [7], [13]. In this paper, we model the interaction between the genuine (player I) and malicious (player II) mesh nodes as a two player non-cooperative, non zero-sum stochastic game with incomplete information.

V. GAME MODEL

In this section we formulate a game to prevent attacks against mesh networks. We consider gray hole attacks, which has been reviewed in the literature [3]. Initially, we present the network model and then discuss the game, the players and their strategies, rewards and costs for the strategies of the players, the transition probability function and the expected utilities.

A. The Forwarding Game

We consider a simple network of 3 mesh routers (a source node S, an Intermediate node B and a destination node D) as shown in figure 1. To transmit the packets to destination node D, the source node S can send packets directly to node D or rely on node B to forward the packets to the destination. In the previous works [10], [11], authors' consider the energy consumption as the important difference between direct and multihop transmission and rely on multihop transmissions for the purpose of preserving energy and reducing interference to other nodes. Does the paths based on low energy consumption, low levels of interference always provide the best results? The answer is no, because the nodes should be able to select the paths that are highly secure in addition to low levels of interference, energy consumption etc. We study the path selection problem from a security perspective and formulate a game in which the source node S selects a secure path as opposed to minimum energy path with higher probability which is the nash equilibrium of this forwarding game.

B. Game Formulation

1) Assumptions: We consider a simple three node network with a malicious node as the intermediate node. In this work, we do not account for packet delay by considering simultaneous transmission and reception possible. In other words, in a single slot the transmission of packet from source S to the destination D can take place via intermediate node B or directly by S. We assume that node B will always accept packets from source node S with probability of 1 because the aim of the malicious node is to pretend as a cooperative node by accepting the request for transmission and then launch the attack on the accepted packet. We also assume that the links are free from wireless errors and hence any dropping in the network is caused by the malicious node.

2) Players: The game discussed in this work is a two-person game and the players in this game are the source node, S, and the intermediate (or malicious) node B. Lets call the source node, S, as player I and the malicious node B as player II. Table I summarizes all the notations used in the formulation of the game.

TABLE I
TABLE OF NOTATIONS

Notations	*Meaning*
S	Source Node and Player I
B	Intermediate Node (Malicious Node) and Player II
D	Destination Node
(m, n)	State of the system
p_d	Probability of forwarding to Destination directly
p_b	Probability of forwarding to Intermediate Node B
q_f	Probability of forwarding the packet by Node B
q_d	Probability of dropping the packet by Node B
μ	Arrival Rate of Packets to Node S
U_s	Utility of Source Node
U_b	Utility of Intermediate Node
R_d	Reward from the destination
R_{sb}	Reward from the Source for B
C_{sd}	Cost of using the path SD
C_{sb}	Cost of using the path SB
C_{bd}	Cost of using the path BD
Π	Steady state probabilities
Q	State Transition Matrix
d	drop buffer
α	Cost of Maliciousness

3) State Space: The state of the game is defined as (m,n), where m is the send buffer of player I and n is the drop buffer of player II. The quantity, m can take values 0 or 1 depending on whether the packet is present in the sending buffer for transmission. For example, if

one packet is present in the send buffer of player I, m, will take a value of 1. The quantity, n, can take values 0 or d, depending on if no packet is dropped or if a packet is dropped. We denote μ as the probability that a new packet arrives at the send buffer of player I. Hence the four possible states of the game are: $k_1 = (0, 0)$, $k_2 = (0, d)$, $k_3 = (1, 0)$, $k_4 = (1, d)$. Since this is a stochastic game with incomplete information, the players have information about their buffers and utilities only and hence the actions of player I will depend on the send buffer m and that of player II will depend on drop buffer n rather than the complete state (m, n).

4) Strategy Space and Mixed Strategies: The player I has two strategies: (a_1) forward the packet directly to destination D, (a_2) forward the packet to D via relay node B. We have strategy set of Player I as $A_I = \{a_1, a_2\}$. The mixed strategies corresponding to A_I are $\pi_s(a_1, a_2)$ = (p_d, p_b), where $p_d + p_b = 1$. p_d is the probability of sending directly to D and p_b is the probability of forwarding the packet via B. In other words, whenever a packet arrives at the send buffer of Player I with probability μ, the player I decides whether to send directly to D with probability p_d or send via B with probability p_b. It is not difficult to see that this happens when the state of the system is ($k_3 = (1, 0)$,$k_4 = (1, d)$). The Player II (attacker) has two strategies: (b_1) forward the accepted packet from player I, (b_2) drop the accepted packet, i.e. we have $B_{II} = \{b_1, b_2\}$. The mixed strategies corresponding to action set B_{II} are $\pi_b(b_1, b_2)$ = (q_f, q_d), where $q_f + q_d = 1$. q_f is the probability of forwarding the accepted packet from S to D and q_d is the probability of dropping the packet maliciously. Clearly, we can see that this happens for states ($k_3 = (1, 0)$,$k_4 = (1, d)$).

5) Costs, Rewards and Utilities: When S sends the packet through the path $S \longrightarrow D$, node S will receive a reward of R_d from destination node, D. When S depends on B for transmitting the packet, it gives a reward of R_{sb} to B for accepting the packet transmission request and receives a reward of R_d from D for successful reception of each packet at D. The reward for S in both cases (sending directly to D and via B to D) comes all the way from destination. Note: Destination was assigned to give the reward to source based on the idea that if S does not receive a reward from destination for the transmitted packet, it can easily identify that the packet did not reach the destination successfully. Each packet transmission from node i to node j incur a path cost of C_{ij}. The cost, C_{ij}, depends on the energy required to use that path, the link quality etc. Node B will receive a profit of α for his malicious dropping of packets. Based on the rewards and costs of the path mentioned above, the nodes S and B will receive the following utilities.

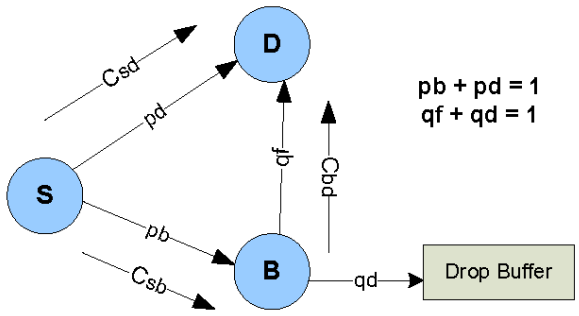

Fig. 1. A simple forwarding game between two players S and B. S is the Source Node, D is the Destination and B is the malicious node. C_{ij} is the cost of path between two nodes i and j. p_b and p_d is the probability of forwarding to B and D. q_d and q_f is the probability of dropping and forwarding.

$$U_s = \begin{cases} R_d - C_{sd} & \text{if } S \text{ transmits directly to } D; \\ R_d - R_{sb} - C_{sb} & \text{if } S \text{ transmits to } D \text{ via } B \\ & \text{and } B \text{ forwards;} \\ -R_{sb} - C_{sb} & \text{if } S \text{ transmits to } D \text{ via } B \\ & \text{and } B \text{ drops.} \end{cases}$$

The utilities are assigned in a such a way that the utility of S will decrease when B drops maliciously compared to the utility it receives when a packet has successfully reached at the destination i.e, $-R_{sb} - C_{sb} < R_d - C_{sd} < R_d - R_{sb} - C_{sb}$.

$$U_b = \begin{cases} R_{sb} - C_{bd} & \text{if } B \text{ forwards the packet to } D; \\ R_{sb} + \alpha & \text{if } B \text{ drops the packet.} \end{cases}$$

The utilities are assigned in such a way that the utility obtained from dropping is higher than utility received from S for forwarding the packets, i.e, $R_{sb} - C_{bd} < R_{sb} + \alpha$.

6) Transition Rule and Expected Utility Functions: It is clear to understand that the state process (m,n) is a two dimensional ergodic markov chain with finite number of states. Lets define ϕ=(π_s, π_b) to be the joint set of random stationary strategies which is given by ϕ = (p_d, p_b, q_f, q_d). Let $\Pi(\phi) = \{\Pi_k(\phi), \forall k \in K\}$ be the steady state probability where its $\Pi_k(\phi)$ factor denotes the proportion of the time that the process will be in state k. Define state transition matrix as $Q(\phi)$ where the entries of the transition matrix denotes the probabilities of transition. The transition probabilities of the markov chain represents the probability of transition from one

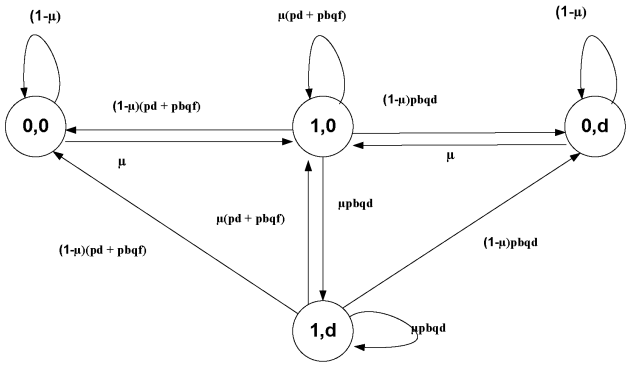

Fig. 2. State Diagram

state to the next state under the joint strategy ϕ and it is expressed as follows:

$\underline{Case\ 1 : m = 1}$

$$P_{(m,n)(m+i,n)}(\phi) = \begin{cases} (1-\mu)(p_d + p_b q_f) & \text{if } i = -1 \\ & n = 0; \\ (1-\mu)(p_b q_d) & \text{if } i = -1 \\ & n = d; \\ (\mu)(p_d + p_b q_f) & \text{if } i = 0 \\ & n = 0; \\ (\mu)(p_b q_d) & \text{if } i = 0 \\ & n = d; \end{cases}$$

$\underline{Case\ 2 : m = 0}$

$$P_{(m,n)(m+i,n)}(\phi) = \begin{cases} (1-\mu) & \text{if } i = 0 \\ & n = 0; \\ (\mu) & \text{if } i = 1 \\ & n = d; \end{cases}$$

The state diagram is shown in figure 2. We can solve for steady state probabilities by using the global balance equation $\Pi(\phi) = \Pi(\phi) \times Q(\phi)$.

To further understand the ideas, we will consider an example. Assume that the current state of the system is $(1, 0)$. The player I has a packet in its send buffer and it can choose any one of the two strategies, transmit directly to D with probability p_d or transmit to player II with probability p_b. If player I transmits to D directly, then the next state of the system will be (0,0) or (1,0). If player I transmits to B and B drops the packet, the next state of the system will be (0,d) or (1,d). If B forwards the packet of source node then the next state will be (0,0) or (1,0).

The expected utilities of the players I and II are calculated as follows:

$$\begin{aligned} U_s(\phi) &= \Pi_{(1,0)}[p_d(R_d - C_{sd}) \\ &+ p_b(q_f(R_d - R_{sb} - C_{sb}) + q_d(-R_{sb} - C_{sb}))] \\ &+ \Pi_{(1,d)}[p_d(R_d - C_{sd}) \\ &+ p_b(q_f(R_d - R_{sb} - C_{sb}) \\ &+ p_b(q_d(-R_{sb} - C_{sb}))] \end{aligned} \quad (1)$$

$$\begin{aligned} U_b(\phi) &= \Pi_{(1,0)}[p_b(q_f(R_{sb} - C_{bd}) + q_d(R_{sb} + \alpha))] \\ &+ \Pi_{(1,d)}[p_b(q_f(R_{sb} - C_{bd}))] \\ &+ \Pi_{(1,d)}(p_b q_d(R_{sb} + \alpha)) \end{aligned} \quad (2)$$

where $\Pi_{(1,0)} = \mu(1 - \mu \times p_b q_d)$, $\Pi_{(1,d)} = \mu^2 \times p_b q_d$.

Note 1: when $(p_b > p_d)$ and $(q_d > q_f)$, the utility of B starts increasing and that of source node S starts decreasing because $\Pi_{(1,d)}$ increases with p_b and q_d and the negative term $p_b q_d(-R_{sb} - C_{sb})$ in U_s starts increasing. But in the case of B, the positive term $(p_b q_d(R_{sb} + \alpha))$ starts increasing with p_b and q_d.

VI. Numerical Analysis

We set the values for costs and rewards as follows: $\mu = 0.5$,R_d = 1, R_{sb} = 0.5, C_{sd} = 0.8, C_{sb} = C_{bd} = 0.1, and α = 0.3. We assume that the direct path has high cost C_{sd} compared to the sum of costs of relaying path (C_{sb} +C_{bd}). In this non-cooperative game between Player I and Player II, we are interested in finding the nash equilibrium strategies ϕ^*=(π_s^*, π_b^*) such that for any player i and any strategy π_i, we have $U_s(\phi^*) \geq U_s(\pi_s, \pi_b^*)$ and $U_b(\phi^*) \geq U_s(\pi_s^*, \pi_b)$. This condition focuses on the requirement of nash equilibrium that each player must be playing a best response against a conjecture. In other words, the best response of player I when player II plays the strategy π_b is $R_I(\pi_b) = argmax_{\pi_s} U_s(\phi)$ and the the best response of player II when player I plays the strategy π_s is $R_{II}(\pi_s) = argmax_{\pi_b} U_b(\phi)$. Hence the nash equilibrium of this non cooperative two-player non-zero sum game would be ϕ^*=(π_s^*, π_b^*) which is given by $\pi_s^* \in R_I(\pi_b^*)$ and $\pi_b^* \in R_{II}(\pi_s^*)$.

Figures $[3-5]$ depicts the utilities of Players I and II with the value of drop probability varying from 0 to 1 for the constant values of p_d and p_b. Figures $[6-9]$ shows the utilities of Players I and II with value of $(p_d + p_b)$ varying from 0 to 1 for the constant value of q_d. Clearly we can see that when $q_d = 0$ and $p_b = 1$, the source node S has the maximum utility of 0.20 and B has a utility of 0.20. But, in this paper we focus on the case when B is malicious and hence it will always drop the packet

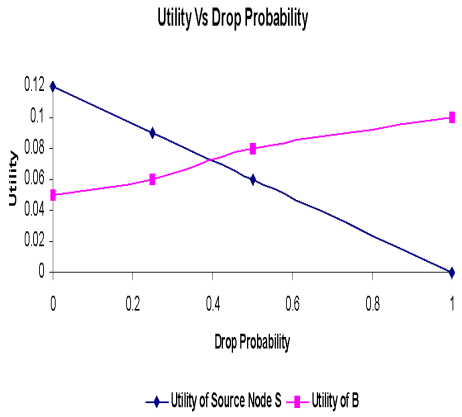

Fig. 3. The utilities of S and B, (U_s, U_b), as a function of q_d for constant value of p_b = 0.25 and p_d = 0.75

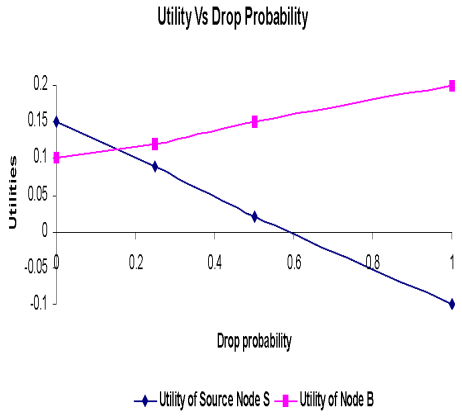

Fig. 4. The utilities of S and B, (U_s, U_b), as a function of q_d for constant value of p_b=p_d = 0.5

with certain probability. As a result B has the maximum utility when $q_d = 1$ and $p_b = 1$. It can be seen from the graphs $(6-9)$ that as the dropping probability (q_d) increases for different values of p_b, player I's utility is less than the utility it receives on selecting pure strategy of direct communication (p_d =1, U_s= 0.10) and as a result player I counteracts by switching to high cost direct communication with probability $p_d = 1$ which is the expected result of this game.

The intuition behind the above discussion is that player I will initially select the minimum cost path with higher probability $(p_b > p_d)$ and player II will always attack the path with certain probability $(q_d \geq q_f$ or $q_d \leq q_f)$ because "attacking" gives it higher utility than "forwarding". As the $U_s(\phi)$ starts decreasing, player I will switch to high cost direct communication path with higher probability $(p_d = 1)$ which is the desired result of this game. Hence the necessary condition for player I to switch to direct communication with higher probability $p_d = 1$ is given by $U_s(p_b, q_d > 0) < U_s(p_d = 1)$. The main aim of this game is to find the best path in terms of security, cost etc.

VII. Conclusions

WMNs gained significant attention because of the numerous applications it supports, e.g., broadband home networking, community and neighborhood networks, delivering video, building automation, in entertainment and sporting venues etc. But the main challenge of these multihop networks is the susceptibility to various security threats. In this paper we study the gray hole attacks in mesh networks and formulate a non cooperative, non zero-sum two player markov game to detect these attacks

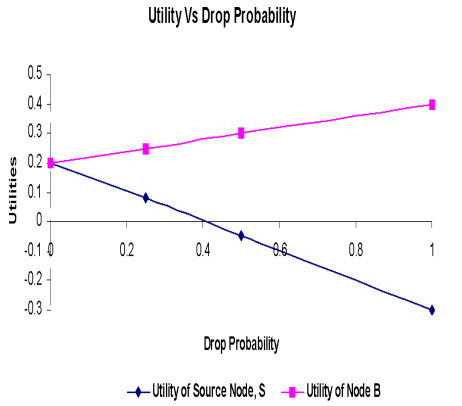

Fig. 5. The utilities of S and B, (U_s, U_b), as a function of q_d for constant value of p_b = 1, p_c=0

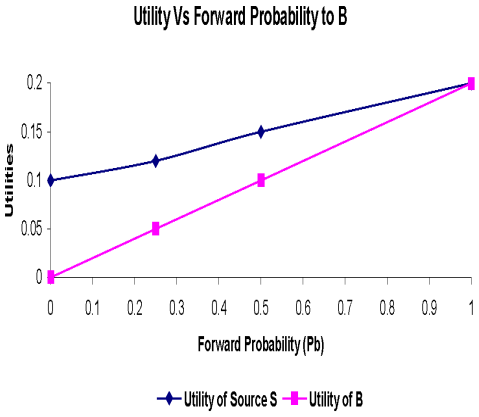

Fig. 6. The utilities of S and B, (U_s, U_b), as a function of p_b for constant value of q_d = 0, q_f =1

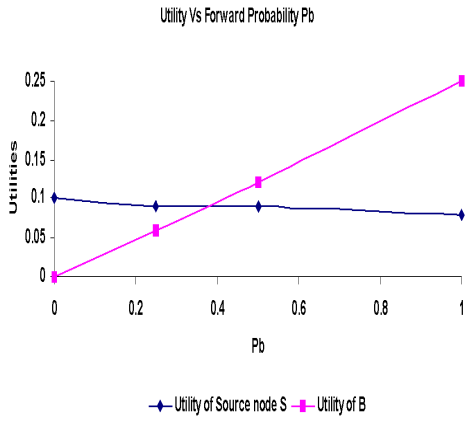

Fig. 7. The utilities of S and B, (U_s, U_b), as a function of p_b for constant value of q_d = 0.25, q_f =0.75

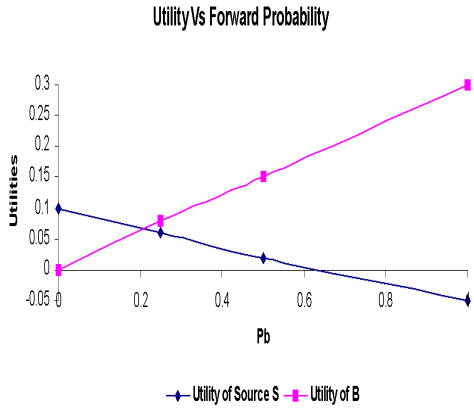

Fig. 8. The utilities of S and B, (U_s, U_b), as a function of p_b for constant value of q_d = 0.5, q_f =0.5

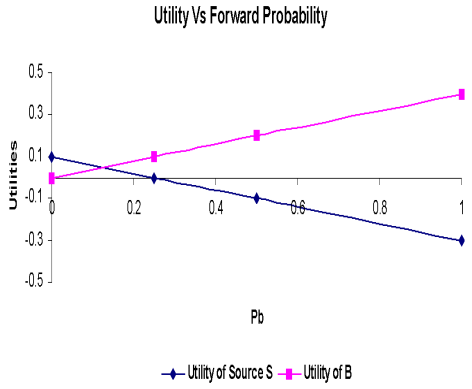

Fig. 9. The utilities of S and B, (U_s, U_b), as a function of p_b for constant value of q_d = 1, q_f =0

and find the best path in terms of security and cost. We saw that when the dropping probability of the attacker increases, the utility of genuine player I decreases and counteracts to this situation by switching to a high cost secure path with higher probability. The main aim of this paper was to show the significant role of security in selecting a path in addition to energy consumption and link quality.

Our future work is to investigate the security issue in a more complex network of mesh routers and relaxing the assumption that any loss of packet in the network is due to the presence of an attacker.

REFERENCES

[1] I.F. Akyildiz and X. Wang, "A survey on Wireless Mesh networks," in *IEEE communication Magazine*, September 2005.

[2] N. B. Salem and J. Hubaux "Securing Wireless Mesh Networks," in *IEEE Wireless Communications*, April 2006.

[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in *First IEEE International Workshop on Sensor Network Protocols and Applications (SNPA 03)*, pp.113-127, May 2003.

[4] B. Xiao, B. Yu and C. Gao "CHEMAS: Identify suspect nodes in selective forwarding attacks," in *Journal of Parallel and Distributed Computing*, pp.1218-1230, June 2007.

[5] D. Manikantan Shila and T. Anjali "Defending Selective Forwarding attacks in WMNs," in *IEEE International Conference on Electro/Information Technology*, 2008.

[6] D. Fudenberg and J. Tirole, "Game Theory," in *MIT Press*, 1991.

[7] P. K. Dutta, "Strategies and Games: Theory and Practice," *MIT Press*, 1999.

[8] A. Patcha and J. Park, "A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks,," *International Journal of Network Security, Vol. 2, No. 2, pp. 146 152*, March 2006.

[9] A. Agah, S. K. Das and K. Basu, "A Non-cooperative Game Approach for Intrusion Detection in Sensor Networks," in *Network Computing and Applications, Third IEEE International Symposium on (NCA'04)*, 2004.

[10] Y. E, Sagduyu and A. Ephremides, "A game theoretic look at simple relay channel," in *Proc. WiOpt'04 (Optimization and Modeling in Mobile, Ad-Hoc and Wireless Networks), Cambridge,UK, March 2004*

[11] J Leino, "Applications of Game Theory in Ad hoc Networks," in Master's thesis, Helsinki University of Technology, *October 2003*

[12] S. M Ross, "Introduction to Probability Models," in Academic Press, *Eighth Edition.*

[13] A. B. MacKenzie and L. A. DaSilva, "Game Theory for Wireless Engineers," Morgan Claypool Publishers' Series, *2006.*