Attacks and Defenses in Mobile IP: Modeling with Stochastic Game Petri Net

Sajedul Talukder
Florida Int’l University
Florida, USA
stalu001@cs.fiu.edu

Md. Iftekharul Islam Sakib
BUET
Dhaka, Bangladesh
miisakib@gmail.com

Md. Faruk Hossen
BUET
Dhaka, Bangladesh
faruk.08.cse@gmail.com

Md. Shohrab Hossain
BUET
Dhaka, Bangladesh
mshohrhossain@cse.buet.ac.bd

Abstract—The urging need for seamless connectivity in mobile environment has contributed to the rapid expansion of Mobile IP. Mobile IP uses wireless transmission medium, thereby making it subject to many security threats during various phases of route optimization. Modeling Mobile IP attacks reasonably and efficiently is the basis for defending against those attacks, which requires quantitative analysis and modeling approaches for expressing threat propagation in Mobile IP. In this paper, we present four well-known Mobile IP attacks, such as Denial-of-Service (DoS) attack, bombing attack, redirection attack and replay attack and model them with Stochastic Game Petri Net (SGPN). Furthermore, we propose mixed strategy based defense strategies for the aforementioned attacks and model them with SGPN. Finally, we calculate the Nash Equilibrium of the attacker-defender game and thereby obtain the steady state probability of the vulnerable attack states. We show that, under the optimal strategy, an IDS needs to remain active 72.4%, 70%, 68.4% and 66.6% of the time to restrict the attacker’s success rate to 8.5%, 6.4%, 7.2% and 8.3% respectively for the aforementioned attacks, thus performing better than the state-of-the-art approach.

I. INTRODUCTION

Wireless communication has witnessed a massive growth in number of users in the recent years. Spreading of wireless networks has influenced everyday life, from e-governance [1] to social networks [2], from digital automation [3] spreading up to space and aeronautical networks [2]. One of the key benefits of wireless technology is mobility, which allows mobile users to move from one network to another while maintaining their home IP address unchanged [5]. Mobile IP (RFC 2002) is a standard protocol established by the Internet Engineering Task Force (IETF) that builds on the Internet Protocol by making mobility transparent to applications and higher level protocols like TCP. Mobile IP settings mostly exist in wireless networks where users need to carry their devices across several networks with different IP address. 3G and 4G networks also use Mobile IP to provide transparency when user of the internet migrates between cellular towers [6]. Mobile IP allows the mobile node to use two IP addresses: a fixed home address and a care-of address that changes at each new point of attachment. Now a days, a vast number of devices are facilitated with Mobile IP that includes Cellular phones, PDAs, GPS, Tablets and other handheld devices. More and more entities getting connected to the wireless networks, the security threats that causes massive impairment are bulging as well. Abundant of malicious nodes that have been thrust into networks across the world have made the detection of Mobile IP attacks more difficult. Network security, in particular Mobile IP security needs to provide confidentiality, availability and integrity for data communication. However, the need to provide an unbroken session as the user or node moves from one link to another without human intervention and non-interactivity has created the scope for the attackers to perform various attacks in Mobile IP. Our study focuses on understanding and modeling the following Mobile IP attacks and their appropriate defense strategies: (1) Denial of Service attack, (2) Redirection attack, (3) Replay attack and (4) Bombing attack. All of the attacks are mostly due to route optimization between the Mobile Node and Corresponding Node. Mobile Node that changes its IP address needs to update its care-of-address and send the binding update to the Corresponding Node. Binding updates are vulnerable to various attacks since Malicious Node can penetrate the route between Mobile Node and Corresponding Node. Attacker can steal information, alter it or redirect it by fooling either Corresponding Node or Mobile Node or both. Researchers have tried to analyze Mobile IP attacks and their defenses using various approaches like using IPSec [7], number of independent data networks [8], nondisclosure method [9], IP security primitives [10], [11], authenticating a mobile node [12], using public-key [13], security association policy server [14] or securing binding update [15]. However, none of the above mentioned works attempted to model and analyze the attacks and defense scenarios using Stochastic Game Petri Net (SGPN). To the best of our knowledge, this paper is the first attempt to model attacks and defenses in Mobile IP using SGPN.

Our Contributions. This paper presents the following contributions:

- **Attack Analysis.** Analyze Mobile IP and four major attacks such as Denial-of-Service (DoS) attack, bombing attack, redirection attack and replay attack present in Mobile IP.
- **Attack Modeling.** Model the attacks using stochastic game petri net (SGPN).
- **Defense Modeling.** Propose mixed strategy based defense strategies for the aforementioned attacks and model them with SGPN.
- **Evaluation.** Evaluate the models by calculating the
steady state probability of the vulnerable attack states and show that, an IDS needs to remain active 72.4%, 70%, 68.4% and 66.6% of the time to restrict the attacker’s success rate to 8.5%, 6.4%, 7.2% and 8.3% respectively for the aforementioned attacks.

The rest of the paper is organized as follows. Section II describes the background of the work. Section III analyzes the previous works. Section IV illustrates the attacks modeling and our proposed solutions to the attacks, Section V deals with the findings and result analysis and finally Section VI concludes the paper with a highlight on the scope of future work.

II. BACKGROUND

A. Mobile IP

IP address is obtained from a TCP connection which uniquely identifies a device/node’s point of attachment to the internet. When a device moves from its home network to a new foreign network, it needs to change its IP address and re-establish a new TCP connection. If there is an ongoing session going on with this device, the session needs to be disconnected until a new IP address of a moving device is obtained. Mobile IP Protocol was proposed by a working group within the Internet Engineering Task Force (IETF) in order to solve this mobility issue. Mobile IP for IPv4 is described in IETF RFC 5944, and extensions are defined in IETF RFC 4721. Mobile IPv6, the IP mobility implementation for the next generation of the Internet Protocol, IPv6, is described in RFC 6275.

1) Mobile IP Overview: Mobile IP designed by IETF is a standard protocol to enable mobile users to move across the network while maintaining their permanent IP address. IP datagram can be routed over Internet transparently using Mobile IP. Each mobile node has a Home Address (HoA) that corresponds to its home network that remains unchanged regardless of its current location. If a node moves to foreign network, it is associated with a Care-of Address (CoA), that provides information of its current location. Using Mobile IP, the device can change its location across various networks without requiring to change its IP address. Home Agent (HA) and Foreign Agent (FA) are the routers that perform the encapsulation and decapsulation of the datagram packets respectively.

2) Mobile IP Terminologies: Now we present the most common terminologies used in Mobile IP.

- **Mobile Node (MN):** A moving device that connects to the internet using a fixed home address and can change the location and point of attachment to the internet while keeping ongoing communication uninterrupted. Examples of MNs are Cellular phones, PDAs, GPS, tablets, routers and other handheld devices.
- **Home Network (HN):** Network within which a MN identifies its home address.
- **Home Address (HoA):** An IP address assigned to MN for a home network that remains same regardless of where the device is attached to the internet.
- **Home Agent (HA):** A router on the MN’s home network that tracks the MN’s current location (CoA), intercept, encapsulates and tunnels datagram packets to the MN when it is away from home.
- **Foreign Network (FN):** Any network other than the MN’s home network, on which MN moves its point of attachment.
- **Care-of-Address (CoA):** A temporary IP address assigned to a MN while it is visiting a foreign network away from its home network.
- **Foreign Agent (FA):** A router on the MN’s foreign network that provides a CoA to the MN and acts as a default router for datagram generated by the MN. It also decapsulates and delivers datagram to the MN that are encapsulated by the MN’s HA.
- **Correspondent Node (CN):** A mobile or stationary device that sends or receives packets to or from the MN.
- **Binding Update (BU):** Message used to notify the HA or CN about the current location of the MN by sending the CoA.

3) Mobile IPv6: In MIPv6, the Mobile Node (MN) can communicate in two ways with the Corresponding Node (CN), through bidirectional tunneling and through route optimization, see figure [1]. In bidirectional tunneling, packets from the CN are sent to the HA, which forwards them to the MN through a tunnel. The MN sends the responses through a reverse tunnel to the HA, which forwards the data to the CN. Communication between MN and CN thus always happens via HA. Whenever, MN changes its network and moves to a new network, it gets a new CoA. MN needs to notify HA about its new CoA and this is done through Binding Update (BU).

Route Optimization. It is possible to bypass the requirement of HA for every packet transfer through the use of route optimization. When route optimization is enabled, any communication after the initial connection through the HA is handled directly between the MN and the CN. A type 2 routing header is used for this process. Since communication occurs...
directly between MN and CN instead of detouring via the HA, it becomes more efficient because routing can be optimized. However, in order to use route optimization, CN must have Mobile IPv6 support on it. Similar to bidirectional tunneling, MN needs to notify CN about its new CoA through BU. Route optimization is one of the main benefits of Mobile IPv6 over Mobile IPv4.

**Return Routability.** In order to prevent redirection attacks during the exchange of BU between MN and CN, an authentication test is needed. This authentication process is called the return routability procedure and lets the CN test whether the MN is actually reachable via both its CoA and its HoA. If the authentication is successful, only then are BU accepted by the CN.

**B. Stochastic Game**

A stochastic game is a n-player game in which players payoff and the probability distribution of a new state being visited depend on the collection of actions that the players choose, together with the current state. A Stochastic Game is represented as a 7-tuple vector

\[ SG = (I, X, A_i, A, r_i, q, \beta), \]

where

1. \( I = \{1, 2, ..., n\} \) is the set of players;
2. \( X = \{1, 2, ..., N\} \) is the state space;
3. \( A_i \) is the finite action set of player \( i \);
4. \( A := A_1 \times ... \times A_n \) is the set of action profiles;
5. \( r_i : X \times \mathbb{R} \rightarrow \mathbb{R} \) is the reward function of a player \( i \); and
6. \( q(x|a) \) is the probability of next state being \( x \)

\[ \text{given that the current state is } x \text{ and the action profile } a \in A; \]
7. \( \beta \in (0, 1) \) is a discount factor.

**C. Petri Net**

Petri net (a.k.a. place/transition net) is a mathematical and graphical modeling language for the description and analysis of concurrent processes in distributed systems. A Petri net is a directed bipartite graph consisting of places, transitions and arcs. Places denote conditions which are represented by rectangular bars. Transitions denote events which are represented by rectangular bars. Arcs run from a place to a transition or vice versa. Arc never runs between places or between transitions. Petri Net is very similar to State Transition Diagrams. Graphically, places in a Petri net may contain a discrete number of tokens. Marking \( M \) is the state of the net at any time in terms of the distribution of tokens over the places. Transitions may be fired to transfer control from input place to output place through the exchange of tokens. A firing is an atomic event.

**III. STOCHASTIC GAME PETRI NET (SGPN)**

We now present the formal representation of Stochastic Game Petri Net (SGPN) which is derived from [16]:

**SGPN.** A SGPN is represented as a 9-tuple vector

\[ SGPN = (N, P, T, F, \pi, \lambda, R, U, M_0), \]

where

1. \( N = 1, 2, ..., n \) is the set of players;
2. \( P \) is a finite set of places;
3. \( T = T^1 \cup T^2 \cup ... \cup T^N \) is a finite set of transitions, where \( T^k \) is the set of transitions with respect to player \( k \) for \( k \in N \);
4. \( \pi : T \rightarrow [0, 1] \) is a routing policy representing the probability of choosing a particular transition;
5. \( F \subseteq I \cup O \) is a set of arcs, where \( I \subseteq P \times T \) and \( O \subseteq T \times P \) such that \( P \cap T = \phi \) and \( P \cup T \neq \phi \), where \( \phi \) is an empty set; we denote \( x = \{y | (y, x) \in F\} \) the preset of \( x \), similarly, \( x = \{y | (x, y) \in F\} \) the post-set of \( x \);
6. \( R : T \rightarrow (R_1, R_2, ..., R_n) \) is a reward function for the players taking each transition, where \( R_i \in (-\infty, +\infty), i \in N \);
7. \( \lambda = \{\lambda_1, \lambda_2, ..., \lambda_w\} \) is a set of transition firing rates in the transition set, where \( w \) is the number of transitions; and
8. \( U \) is the utility function of players; and
9. \( M_0 \) is the initial marking.

Each token \( s \) is assigned a reward vector

\[ h(s) = (h_1(s), h_2(s), ..., h_n(s)) \] as its property, where \( h_k(s) \) is the reward of player \( k \) in token \( s \). Players get the reward \( R(t) \) after the firing of the transition \( t \) and the reward is recorded in the reward vector \( h(t) \) of the token [16]. For the sake of simplicity and to fit our attacker-defender model, we assume that our stochastic game is a two-player discounted stochastic game.

**Definition 1 (Transition Probability Matrix).** Given a SGPN with \( r \) places, a Transition Probability Matrix is a \( r \times r \) matrix \( M \), where \( M_{ij} \) represents the probability of a transition \( t_k \) being fired such that \( p_i \) is the input place, \( p_j \) is the output place and \( p_i, p_j \in P, t_k \in T \).

**Definition 2 (Strategy).** Given a player \( k \) in SGPN, strategy is a vector \( \pi_k = (\pi_{(1)}, \pi_{(2)}, ..., \pi_{(w)}) \), where \( \pi_{(w)} \) is the probability that player \( k \) takes action \( t_j \) and \( w_j = | T^k | \).

**Definition 3 (Utility).** Given a SGPN in infinite time horizon with \( n \) players, utility of a player \( i \) is

\[ U_i(p, \pi) = \sum_{k=1}^{\infty} \beta^{k-1} R_i^k(p, \pi), \]

where \( \pi = (\pi_1, \pi_2, ..., \pi_n), \beta \in (0, 1) \) is a discount factor and \( R_i^k(p, \pi) \) is the expected reward function of player \( i \) at the \( k \)-th stage of the game. It can be further simplified to \( U_i^*(\pi) \) when \( p \) denotes the initial state of player \( i \).

**Definition 4 (Nash Equilibrium).** Given a SGPN, a Nash Equilibrium for a two-player stochastic game is a vector profile \( \pi^* = (\pi^*_1, \pi^*_2, ..., \pi^*_n) \) such that \( U_i(p, \pi^*) \geq U_i(p, \pi_i, \pi_{-i}^*) \) for all \( p \in P, i \in N \), where \( \pi_{-i}^* \) is any alternative mixed strategy of player \( i \) except \( \pi^* \).

**Theorem 1.** Every discounted stochastic game is guaranteed to have a Stationary Nash Equilibrium.

**Proof.** Let \( F_i = (f_{i1}, f_{i2}, ..., f_{in}) \) be the set of stationary strategies for player \( i \).
A Stationary Nash Equilibrium belongs to the class of strategy profiles $F^1 \times \ldots \times F^n$. We need to prove that, there exists $f^* = (f^*_1, f^*_2, \ldots, f^*_n) \in F$ such that $U^i(p, f^*) \geq U^j(p, \pi_i, f^*_i)$ for all $p \in P$ and $i \in N$.

We note that $F$ is a compact convex set in some Euclidean space. We also observe that $U^i(p, \cdot)$ is continuous on $F$.

We get,

$$ (f^*_1, f^*_2, \ldots, f^*_k) \Rightarrow (f_1, f_2, \ldots, f_n) \text{ as } k \to \infty $$

$$ \Rightarrow U^i(p, f^*_1, \ldots, f^*_k) \to U^i(p, f_1, \ldots, f_n) \quad (1) $$

Equation (1) follows directly from the formula:

$$ U^i(f_1, \ldots, f_n) = (N - \beta Q f_1, \ldots, f_n)^{-1} R_i(f_1, \ldots, f_n) $$

where $Q$ denotes the probability of the next state given the current state.

Claim. A policy $f^* = (f^*_1, f^*_2, \ldots, f^*_n)$ is a Nash Equilibrium if $U^i(\cdot, f^*)$ satisfies the following optimality equation:

$$ U^i(p, f^*) = R_i(p, f^*) + \beta \sum_{x \in P} U^i(x, f^*)Q(x | p, f^*) $$

for all $p \in P$ and $i \in N$.

IV. RELATED WORK

Inoue et al. [10] present an implementation example of a secure mobile system which employs a secure mobile IP protocol on stationary security gateways and mobile hosts by modifying IETF standard Mobile IP protocol with IP security primitives, which control the packet flow from a mobile host through multiple security gateways.

Braun et al. [11] describe a solution called secure mobile IP (SecMIP) to provide mobile IP users secure access to their company’s firewall protected virtual private network by making a slight adaptation of the end system communication software in order to adapt the mobile IP and IP security protocol implementations to each other.

Leung [12] provides methods and apparatus for authenticating a mobile node by configuring the server to provide a plurality of security associations associated with a plurality of mobile nodes.

Zao et al. [13] present the design and the implementation of a public key management system called Mobile IP Security (MoIPS) built upon a DNS based X.509 Public Key Infrastructure and the innovation in cross certification and zeromessage key generation that can be used with IETF basic and route optimized Mobile IP.

Yokote et al. [14] present a solution to asynchronous security association between nodes by implementing a security association policy server for IPsec in third generation and beyond wireless mobile access, Internet protocol-based digital networks supporting Mobile IP.

Deng et al. [15] point out the weaknesses of two solutions proposed by the IETF Mobile IP Working Group and present a new protocol for securing binding update messages in order to defend against redirection attack.

Hossain et al. [17] explain with illustrative examples major security threats and several existing security solutions on various components of the network involving the mobility and identified additional security holes of these existing solutions and propose some simple mechanisms to counter them.

Lin et al. [18] propose Stochastic Game Nets (SGN) to model and deal with the game issues, which takes advantages of both stochastic game theory and Stochastic Petri Nets by inheriting the flexible modeling approach of Stochastic Petri Nets. They also apply the SGN method to model and analyze the network attacks, compute the Nash Equilibrium and best-response strategies to defend the attacks. A number of researchers [19]–[27] have proposed game-theory based solutions for network security problems. However, Lin et al. [18] propose Stochastic Game Nets (SGN) to model and deal with the game issues, which takes advantages of both stochastic game theory and Stochastic Petri Nets by inheriting the flexible modeling approach of Stochastic Petri Nets. They also apply the SGN method to model and analyze the network attacks, compute the Nash Equilibrium and best-response strategies to defend the attacks. Wang et al. [16], [28] later extended this work by applying it to the security analysis for enterprise networks. Our work extends the work of [16], [28] but differs in the fact that while they applied Stochastic Game Net (SGN) to model attacks in enterprise networks, we apply Stochastic Game Petri Net (SGPN) to model attacks and defenses in Mobile IP.

V. SGPN REPRESENTATION

We represent our SGPN models according to the following graphical rules: Each place in the Petri Net is represented by the round red colored circles with having the label inside the circle. Each transition in the Petri Net is represented by rectangular red colored shapes with having label placed inside the rectangle. All the arcs are represented by the directed arrows resembling the actual arcs. Figure 2 shows an example how the Petri Nets are converted in the SGPN.

VI. ATTACK MODELING

A. Denial of Service (DoS) Attack

Denial-of-Service (DoS) is an attack that makes a device or web resource temporarily or indefinitely inaccessible to its
authorized users. In Mobile IPv4, DoS attacks is performed by the preclusion of packets from flowing between two nodes. DoS attacks are very common in target sites or services hosted on high-profile web servers such as business sites, credit card payment gateways, banks, and even root name servers. DoS attack is also possible in IPv6. Since the IPv6 support is on par with the IPv4-based feature set, attacks can be carried out over IPv4, and by shifting over to IPv6 it is possible to bypass the defenses that only inspect IPv4 traffic. Generally saying, DoS attack takes the following steps:

- In order to initiate the attack, the attacker stays on the path between two nodes to perform the preclusion of packets flowing between them by intercepting the communication between the two nodes directly.
- When a mobile node is connected on the foreign network, it must use the registration request to inform its home agent of its current care-of address. Home agent intercepts and tunnels all the traffic destined to mobile nodes home address to its Care-of-Address (CoA).
- During the attack, the attacker creates a bogus Registration Request, specifying his own IP address as the CoA for the mobile node.
- If the mobile node’s home address is fooled by this fake registration request, all packets would be tunneled to the attacker instead of mobile node’s actual CoA. Thus, the connection to the mobile node is lost.

B. Redirection Attack

Redirection attack is a type of attack in which the intended traffic for the MN is redirected by the attacker through sending a fabricated BU, thus depriving MN from getting data. To launch the redirection attacks, the IP addresses of the communicating nodes has to be known by the attacker. Hence, nodes with well-known IP addresses, such as file servers, public servers and DNS servers are more vulnerable to such attacks. The attack takes place in the following steps:

- The attacker sends a fake binding update message to CN claiming that the MN has changed its care-of address due to its movement to a new location.
- If the BU is not authenticated, it will be accepted by the CN. CN will now start sending packets to the new CoA which is fake and the MN will not get any traffic.

| Place | Description |
|-------|-------------|
| State 1 | Attacker is ready |
| State 2 | Attacker has collected IP addresses of MN and CN |
| State 3 | Attacker has created fabricated BU |
| State 4 | CN has updated binding cache using wrong IP address |
| State 5 | CN is ready to send data |
| State 6 | CN has sent data to wrong CoA |

| Transition | Description |
|------------|-------------|
| Collect IP Addresses of MN & CN | Attacker is collecting IP addresses of MN & CN |
| Create Fabricated BU | Attacker is creating fabricated BU |
| Req to Update Binding Cache | Attacker is requesting to update the binding cache with its fake BU |
| Send Data to New CoA | CN is sending data to wrong CoA |
| Back to Ready | CN is getting back to ready to send data again |
**C. Bombing Attack**

Bombing attack is an attack where large amount of unwanted data traffic is redirected to the victim node to degrade its performance as well as bandwidth wastage. The attacker may exploit real-time streaming servers for this kind of attack. The attack is performed through the following steps:

- First, the attacker establishes a connection with streaming server, and request to download a large stream of data.
- Once the server accepts the request, the attacker starts to get the data along with the sequence number of the data packets. After getting the initial sequence number, the attacker might claim that it has moved to a new location. The attacker uses the IP address of the victim MN in the binding update.
- As a result, subsequent packets from the server will be directed to the victim node causing its performance degradation and bandwidth wastage of the MN.

**D. Replay Attack**

Replay attack is a type of attack that takes the advantage of a previously recorded binding update by replaying it when the victim (MN) moves to some new location, thereby disrupting the communication between the CN and the MN. Replay attack works by the following steps:

- The attacker stays in close proximity to the MN or CN, for example being in the same radio access network. Thus, the attacker has the ability to record any BU send by the MN to the CN.
- When MN moves to a new network, it sends a BU to the CN. The attacker listening to such BU records the BU to use for replay attack in future.
- When the MN moves to another new location, the attacker replays the recorded BU to the CN to trick CN. If the CN accepts such replay message, it would start sending packets to the old address thinking that MN has again moved to the old address. Thus, traffic from CN are redirected to a non-existing IP-address, thereby interrupting the communication to the MN.
VII. DEFENSE MODELING

A. Denial of Service (DoS) Defense

The defense for the DoS attack is simply to prevent bogus registrations by the attacker. This can be done by imposing strong authentication on all registration traffic exchange between a mobile node and its home IP agent. Under the assumption that the shared secret key is protected, this can ensure that the traffic intended for mobile node is inaccessible to the attacker. All implementation of Mobile IP supports the default algorithm MD5 for authentication, however mobile node and home agent can use any authentication algorithm they agree upon.

B. Redirection Defense

In order to defend against the redirection attack, CN should authenticate the BU before updating it. CN should send data to the new location only when the BU is authenticated. Another mitigation to this problem could be frequently changing the IP address by the communicating nodes. However, this is impractical since this additional security mechanism will make the mobility protocol slower and more complex. Brief description about the states and the transitions for solution scenario of redirection attack are given below-

C. Bombing Defense

For defending against bombing attack, server can send a hello packet to the new location and wait for the acknowledgement. After receiving acknowledgement from the new location, server will send the desired data to MN. Thus, bombing attack can be prevented. However, one possible problem of this defense is that, the attacker can spoof acknowledgement to the server as it knows the initial sequence number making a continuous flow of data streams sent to the victim. One possible solution of this could be to use the TCP RESET signal by the victim node to immediately stop such flow of data stream.

D. Replay Defense

In order to defend against the replay attack, CN should authenticate the BU before updating it. However, it is very difficult to defend against replay attack since the attacker is already using some authenticated BU. On possible solution for this problem is to use the sequence number as the authentication parameter. CN should store the sequence number of the previously send binding updates in a stable storage. CN
should send data to the new location only when the BU is authenticated and the sequence number is not repeated.

VIII. Evaluation

We now evaluate our modeling approach by calculating the steady state probabilities of the attack and defense scenarios. We compare the infection probability of the attacks and our proposed defense scenarios. We use simulation technique using MATLAB to get the probability values and for plotting the simulation data. We use algorithm 1 to calculate the steady state probability from the Nash Equilibrium.

Algorithm 1 Evaluate SGPN Model
1: Let, $\{A_n^i, D_n^i\}, \{A_n^a, A_n^d\}, \{D_n^1, D_n^2\}$ and $\{D_1^1, D_2^2\}$ be the reward values for the attacker’s attack, attacker’s not attack, defender’s defend and defender’s not defend actions respectively.
2: $P_A \leftarrow$ Attacker’s probability of Attacking
3: $P_D \leftarrow$ Defender’s probability of defending
4: Calculate $NE \leftarrow \{P_A, P_D\}$ by solving the following:
5: $P_A \times A_1^1 + (1 - P_A) \times A_1^2 = P_A \times D_1^1 + (1 - P_A) \times D_1^2$
6: $P_D \times A_2^2 + (1 - P_D) \times D_2^2 = P_D \times A_2^1 + (1 - P_D) \times D_2^1$
7: $M_e \leftarrow$ Reduced attack-defend model
8: Generate reachability tree, $T_e$ from the attack-defend model, $M_e$
9: Calculate steady state probability, $\pi$ using $T_e$
10: We can say that, if defender defends $P_D\%$ of the time, the probability of a successful attack is $\pi\%$

In the simulations, we have used the following reward values for the attacker and defender that can be summarized in Table I.

### A. Steady State Probabilities

We now calculate the steady state probabilities of the attack models. For that we have generated the reachability trees from the models. For the simplicity of calculation, we have reduced the models by keeping the attack-defend states and removing the non attack-defend states. Figure 12 shows an example of the reduced attack-defend model of the replay attack defense. Figure 13 shows the reachability tree generated from the attack-defend model of the replay attack defense.
Using the reward values from Figure 11 for replay attack, we can calculate the Nash Equilibrium for the replay attack defense. Plugging in the values, $A_1^a = -0.3, A_1^n = 0.6, D_1^d = 0, D_1^n = 0, A_2^a = -0.15, D_2^d = -0.15, A_2^n = -0.6, D_2^n = 0$, we get the NE = $\{0.25, 0.6667\}$. By using the reachability tree and NE probabilities, we get the following steady state probabilities $\{\pi_9, \pi_{10}, \pi_{11}\} = \{0.75, 0.08333, 0.16667\}$. From the above calculations, we can say that if the defender defends 66.67% of the time, the probability of a successful attack is only 8.333%.

In a similar fashion, we calculate the NE and steady state probabilities of the remaining attacks: DoS attack, bombing attack and redirection attack. We find the values of $P_D$ as 0.724, 0.70 and 0.684 respectively. From these, we find the values of steady state probabilities as 0.0857412, 0.0642 and 0.07287 respectively. Thus, we can conclude that under the optimal strategy, an IDS needs to remain active 72.4%, 70%, 68.4% and 66.6% of the time to restrict the attackers success rate to 8.5%, 6.4%, 7.2% and 8.3% for the Denial-of-Service (DoS) attack, bombing attack, redirection attack and replay attack respectively.

B. Comparison with state-of-the-art approach

Our model performs better than many state-of-the-art approaches for intrusion detection in wireless networks using game theory. Though the other researchers have performed their analysis in a slightly different contexts, we believe our work is comparable to them. For example, Ma et al. [29] has shown that their approach can detect the attacker in 70% to 85% of the cases. In other words, the attacker is able to perform successful attacks in 15% to 30% cases. In our case, on average the attacker is able to perform successful attack only in 7.6% of the cases. In other words, IDS can detect the attacker over 92% of the cases. Similar comparisons can also be drawn with other intrusion detection approaches modeled with game theory.

IX. Conclusions

In our works, SGPN bring together the Game Theory and the Stochastic Petri Nets, and thus takes the gains of both stochastic game theory and Stochastic Petri Nets. It is our strong believe that the proposed SGPN approach can unwrap a new possibility to deal with the security issues in wireless and communication networks. We show that under the optimal strategy, our model can restrict the attackers success rate to 8.5%, 6.4%, 7.2% and 8.3% for the Denial-of-Service (DoS) attack, bombing attack, redirection attack and replay attack respectively. The IDS needs to remain active only 72.4%, 70%, 68.4% and 66.6% of the time to achieve such performances. Future networks will rely on autonomous and distributed architectures to improve the competence and suppleness of mobile applications, and our SGPN provides the ideal framework for designing efficient and robust distributed algorithms.

X. ACKNOWLEDGMENT

The authors would like to thank Dr. Bogdan Carbunar for his valuable advice and guidance.
REFERENCES

[1] S. K. Talukder, M. I. I. Sakib, and M. M. Rahman, “Model for e-government in bangladesh: A unique id based approach,” in 2014 International Conference on Informatics, Electronics Vision (ICIEV), May 2014, pp. 1–6.

[2] S. Talukder and B. Carbunar, “When friend becomes abuser: Evidence of friend abuse in facebook,” in Proceedings of the ACM WebSci, 2017.

[3] S. K. Talukder, M. I. I. Sakib, and M. M. Rahman, “Digital land management system: A new initiative for bangladesh,” in 2014 International Conference on Electrical Engineering and Information Communication Technology, April 2014, pp. 1–6.

[4] K. Leung, D. Shell, W. D. Ivancic, D. H. Stewart, T. L. Bell, and B. A. Kachmar, “Application of mobile-ip to space and aeronautical networks,” in 2001 IEEE Aerospace Conference Proceedings (Cat. No.01TH8542), vol. 2, 2001, pp. 2/027–2/1033 vol.2.

[5] C. So-In, “Mobile ip survey,” 2006.

[6] W. Song, W. Zhuang, and A. Saleh, “Interworking of 3g cellular networks and wireless lans,” International Journal of Wireless and Mobile Computing, vol. 2, no. 4, pp. 237–247, 2007.

[7] A. Yokote, “Method for implementing ip security in mobile ip networks,” Apr. 6 2001, uS Patent App. 09/827,632.

[8] H. Haverinen, J.-P. Honkanen, and A. Kuikka, “Ip security and mobile networking,” Apr. 9 2002, uS Patent App. 10/019,509.

[9] A. Fasbender, D. Kesdogan, and O. Kubitz, “Variable and scalable security: Protection of location information in mobile ip,” in Vehicular Technology Conference, 1996. Mobile Technology for the Human Race., IEEE 46th, vol. 2. IEEE, 1996, pp. 963–967.

[10] A. Inoue, M. Ishiyama, A. Fukumoto, and T. Okamoto, “Secure mobile ip using ip security primitives,” in Enabling Technologies: Infrastructure for Collaborative Enterprises. 1997. Proceedings., Sixth IEEE Workshops on. IEEE, 1997, pp. 235–241.

[11] T. Braun and M. Danzeisen, “Secure mobile ip communication,” in Local Computer Networks, 2001. Proceedings. LCN 2001. 26th Annual IEEE Conference on. IEEE, 2001, pp. 586–593.

[12] K. K. Leung, “Mobile ip authentication,” Jul. 6 2004, uS Patent 6,760,444.

[13] J. Zao, J. Gahm, G. Troxel, M. Condell, P. Helinck, N. Yuan, I. Castineyra, and S. Kent, “A public-key based secure mobile ip,” Wireless Networks, vol. 5, no. 5, pp. 373–390, 1999.

[14] A. Yokote, “Intelligent security association management server for mobile ip networks,” Apr. 3 2002, uS Patent App. 10/114,695.

[15] R. H. Deng, J. Zhou, and F. Bao, “Defending against redirect attacks in mobile ip,” in Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002, pp. 59–67.

[16] Y. Wang, J. Li, K. Meng, C. Lin, and X. Cheng, “Modeling and security analysis of enterprise network using attack–defense stochastic game petri nets,” Security and Communication Networks, vol. 6, no. 1, pp. 89–99, 2013.

[17] M. S. Hossain, M. Atiquzzaman, and W. D. Ivancic, “Security vulnerabilities and protection mechanisms of mobility management protocols,” in Aerospace Conference, 2011 IEEE. IEEE, 2011, pp. 1–12.

[18] C. Lin, Y. Wang, Y. Wang, H. Zhu, and Q.-L. Li, “Stochastic game nets and applications in network security.”

[19] P. Michiardi and R. Molva, “Game theoretic analysis of security in mobile ad hoc networks,” 2002.

[20] T. Alpcan and T. Basar, “A game theoretic approach to decision and analysis in network intrustion detection,” in Decision and Control, 2003. Proceedings. 42nd IEEE Conference on, vol. 3. IEEE, 2003, pp. 2595–2600.

[21] A. Agah, S. K. Das, and K. Basu, “A game theory based approach for security in wireless sensor networks,” in Performance, Computing, and Communications, 2004 IEEE International Conference on. IEEE, 2004, pp. 259–263.

[22] K.-w. Lye and J. M. Wing, “Game strategies in network security,” International Journal of Information Security, vol. 4, no. 1-2, pp. 71–86, 2005.

[23] A. Agah and S. K. Das, “Preventing dos attacks in wireless sensor networks: A repeated game theory approach.” IJ Network Security, vol. 5, no. 2, pp. 145–153, 2007.

[24] Y. Luo, F. Szidarovszky, Y. Al-Nashif, and S. Hariri, “Game theory based network security,” Journal of Information Security, vol. 1, no. 01, p. 41, 2010.