Tackling Intruders in Wireless Mesh Networks

Al-Sakib Khan Pathan, Shapla Khanam, Habibullah Yusuf Saleem, and Wafaa Mustafa Abduallah

Department of Computer Science, International Islamic University Malaysia (IIUM), Gombak 53100, Kuala Lumpur, Malaysia

Abstract

This chapter presents a different approach of tackling intruders in Wireless Mesh Networks (WMN). Traditional approach of intruder detection and prevention suggests purging out intruders immediately after their detection. In our work, we take a different approach to tackle intruder rather than purging it out of the network unless it is marked as a direct threat to the network's operation. Our intrusion tackling model is termed '*Pay-and-Stay*' (PaS) model which allows a rogue node to stay in the network only with the expense of doing some traffic forwarding tasks in the network. Failing to carry out the required tasks of packet forwarding disqualifies the node permanently and eventually that rogue entity is purged out. Alongside presenting our approach, we briefly talk about other available literature, essential knowledge on wireless network intrusion detection and prevention, and status of intrusion related works for WMN.

1. WMN Intrusion Tackling Schemes: The Background

Wireless Mesh Network (WMN) [1], [2] has become a very popular front of research in the recent days. However, as a type of wireless network, it has several weaknesses that are usually associated with any kind of *wireless* technologies. Unlike its wired counterpart, due to the use of wireless communications, secure authentication with access control and various security issues are very crucial in such type of network to ensure proper service to the legitimate users alongside preventing a variety of attacks. Most of the security threats are posed by the illegitimate entities that enter or intrude within the network perimeter, which could be commonly termed as *intruders*. Sometimes a legitimate node could also be compromised in some way so that an attacker-intended task for '*security breach*' could be performed. We, in this chapter, term any such kind of rogue node or entity as an *intruder*. So, the main objective of this work is to identify any kind of intrusion in a WMN and tackle it in a meticulous manner so that a wide range of security attacks could be deterred as well as the network could be benefited. As we will go

through the chapter, we will explain the concepts and motivations behind our approach of dealing with this issue.

1.1. WMN Architecture and Related Background

The mesh architecture of wireless network concentrates on the emerging market requirements for building networks that are highly scalable and cost effective. However, wireless mesh networks lack efficient security guarantees in various protocol layers [3], [4]. There are a number of factors that come into the consideration. Firstly, all communications go through the shared wireless nodes in WMNs which make the physical security vulnerable. Secondly, the mesh nodes are often mobile, which move to different directions and often change the topology of the network. Finally, since all communications are transmitted via wireless nodes, any malicious node can provide with the misleading topology updates and those updates could spread out over the whole network topology [5], [6]. All these points make it difficult to ensure proper level security. However, it is intended to achieve at least some kind of agreed upon standard for a particular application scenario by identifying the rogue entities within the network. That is why we believe; detecting rogue node (intruder, thus an intrusion event) and tackling the intruder skillfully can keep away different kinds of attacks and keep the network healthy for its proper operations.

1.2. A Different Perspective of Tackling Intrusion in WMN

WMNs consist of mesh routers and mesh clients, where mesh routers form the backbone of the network that provides network access to both the mesh and conventional clients. Mesh clients can either connect (see Figure 1) to a backbone or among each other. Hence, mesh client can access the network through the mesh router in a multi-hop fashion. Therefore, any malicious node or intruder can attack the network in the forms of blackhole attack, grayhole attack, Sybil attack, and so on [1], [5]. In all of these attacks, the routing packets are deliberately misled towards wrong destinations or network entities. Once the malicious node (here, we will call it as *intruder*) has control over the packet after getting it in its trap, the packet could be modified, fabricated, dropped, or forwarded (arbitrarily); all of which are considered major obstacles for secure and guaranteed routing in WMN. Our idea is that in such attack scenario, we will allow the node to operate but for its actions, it needs to pay in a high-scale so that it is deterred from doing further mischief. We call our approach as '*Pay-and-Stay*' (PaS) model of intruder tackling as the intruder needs to pay for its stay once it sets itself within the network. We will illustrate how we achieve our goal in the later sections. It should be noted here that we focus on the modeling of intruder/intrusion detection and its efficient tackling; hence, other issues like physical layer issues, transmission and channel

or signal related issues, core routing issues, cryptographic and key management issues, etc. are out of the scope of this work.

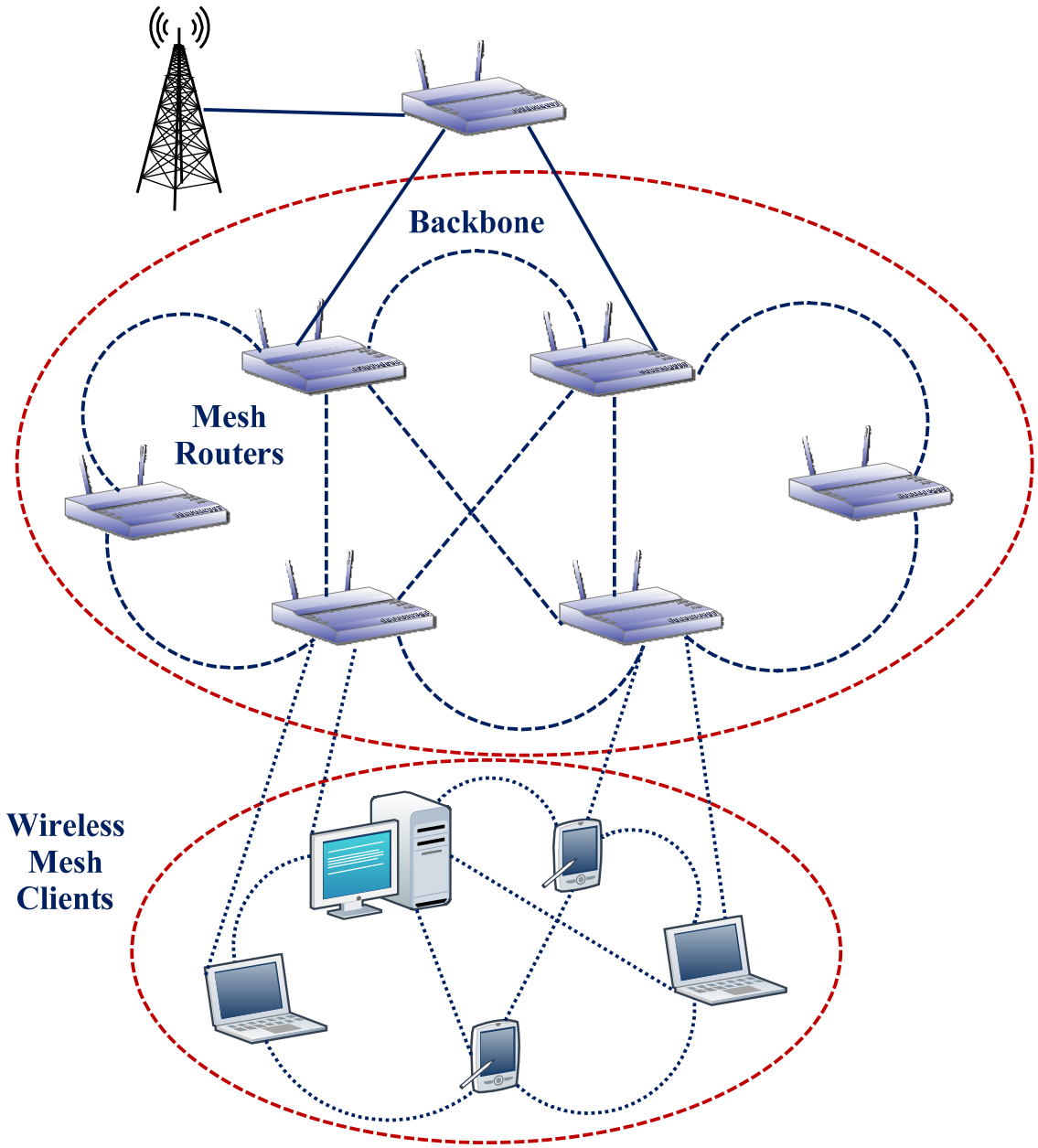

Figure 1. Hybrid Wireless Mesh Network.

1.3. Status of IDS and IPS for Wireless Mesh Networks

IDS (Intrusion Detection System) or IPS (Intrusion Prevention System), both fields are insufficiently researched in case of wireless mesh networks. As this type of network has a mesh backbone which could have devices with proper amount of resources and considerably high energy supply, the usual intrusion detection and prevention mechanisms could be often applied on the basic structure/backbone. However, the problem arises when we want to tackle intrusions in the end-user level (mesh clients or fringe portion). Figure 1 shows a typical structure of WMN, where we show the mesh clients in the network.

The mesh clients could be consisted of different types of devices ranging from a laptop to a mobile phone; even wireless sensor network (WSN) could be at the mesh network end as mesh clients. Any effective intrusion tackling mechanism for WSN could be difficult to implement on the sensors because of their lack of proper resources and this matter is treated as a separate research issue, which is out of the scope of this work. For other types of mesh clients, some kind of intrusion tackling mechanism can be employed. Our work mainly focuses on this area, where a different approach of tackling intrusion could end up as beneficial for the network by allowing an intruder to stay in the network rather than instantly purging it out once it is caught or marked. This matter will be discussed further in the chapter.

1.4. Current Status of Achievements and Our Motivation

Till today, the works on intrusion in WMN are very scarce. Often the proposed approaches do not offer any good solution of the problem but rather put some kind of scratchy overview. There are a few other works which could also be mentioned as they provide important information and ideas related to the field. Hence, in this sub-section, we present the notable past works especially focusing on this topic and also some other works which are somewhat related to our approach.

RADAR is a reputation-based scheme for detecting anomalous nodes in WMN presented in [7]. The authors use the concept of reputation to characterize and quantify the mesh node's behavior and status in terms of some performance metrics. The RADAR architecture shows how the reputation of network nodes is maintained. The reputation management is defined as a feedback process that involves the monitoring and tracking of a mesh node's performance and the evaluation reports from the witnesses. A trust network construction algorithm is also presented and performance is measured taking some critical parameters like false positive, decision accuracy, response latency, and detection overhead. The idea of using reputation is not very different than those are used in available literatures in other fields, but the

way the authors formed their algorithm and architecture for WMN, is proven to be effective for some scenarios.

[8] describes an architecture of asymmetric distributed and cooperative intrusion detection system for WMN. In this work, authors mention the notion of selfish behavior of suspected intruder. They use a double-mode mechanism in the detection model for judgment of troubling behavior: (a) the frequency of node's seizing channel behavior during the active time of the node, (b) continuous sampling result of node's back-off value. Alongside presenting the idea in mathematical form, the authors put an analysis of the whole scheme in terms of throughput ratio and detection delay.

The idea of [9] is to note down various basic information about intrusion detection in WMN and to propose an IDS architecture. This work however, is very elementary and the authors also note that they put forward an initial design of a modular architecture for intrusion detection, highlighting how it addresses their identified challenges. [10] presents an IDS software prototype over a wireless mesh network test-bed. The authors implement the idea and the evaluations are presented in limited range. This work is however incomplete, as there are lots of unanswered questions like what to do with a distributed or large scale WMN, what to do to ensure real-time analysis and detection of anomalous nodes, etc.

OpenLIDS is a lightweight IDS for WMN presented in [11]. This work shows an analysis of a typical wireless mesh networking device performing common intrusion detection tasks. The authors examine the participating nodes' ability to perform intrusion detection. The experimental study shows that commonly-used deep packet inspection approaches are unreliable on typical hardware. So, the authors implement a set of lightweight anomaly detection mechanisms as part of an intrusion detection system, called OpenLIDS. They also show that even with the limited hardware resources of a mesh device, it can detect current malware behavior in an efficient way.

[12] presents a very simple model of intrusion detection in WMN. This work is questionable as the contribution is limited to a vague work-flow diagram with insufficiently done analysis. However, from the objective mentioned in the work, it is understood that the authors targeted designing only a framework without going into any details of the operations. [13] presents an idea of using finite state machine to model intrusion detection in wireless mesh networks. By simulation studies, the authors show that under flooding-combined attack, the IDS shows high false alarm rate due to the side-effect of flooding on attacker's neighbors. Hence, the dummy node used in the approach needs more design features to record

more information about the monitored node. This work is flawed and a convincing result is yet to be achieved.

In [14], the authors present a framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks. Some intrusion detection agent structures are shown. The concept is shown mainly in the forms of some diagrams and flow-charts where different components work in a cooperative fashion. The idea however, looks not very well-baked and somewhat naive. The work presents the primary components (or, agents) that should be installed in mesh routers and mesh nodes. Detection of intrusion could be made and an action database could be used for making decision about any detected intruder. No detailed analysis is presented in the work and it basically touches the surface of the problem.

As evident from the above mentioned works on IDS in WMN, very few countable papers have been published so far on this topic. Again, none of the above works talked about intrusion tackling or utilizing the intruder for the network's benefit before purging it out. Hence, we have come up with the idea of intrusion tackling by *PaS* model. While the proposal section could outline the details of the model, here are more related works that inspired or influenced our way of thinking to build up the basic mathematical and theoretical intrusion tackling model.

In [3], the authors propose an algorithm to specifically defend against security attacks in WMNs where the algorithm makes use of counter threshold to find threshold value. This threshold value will be compared with the actual number of data packets delivered. If the actual data packet is less than the threshold value, then the route is declared to contain malicious node(s) which implies the packet loss is always due to the malicious node(s). Therefore, the path will be excluded from route selection. However, the packet loss may occur due to other factors such as mobility and battery power. If we keep excluding the route by assuming that the poor performance routes contain malicious nodes, then we may end up with few routes or no routes for communications at the end. This method may work on specific settings but is not efficient to encounter security attacks in dynamic topologies of WMNs.

The authors in [15] advocate using PANA (Protocol for carrying Authentication for Network Access), to authenticate the wireless clients. The PANA model also provides the cryptographic materials necessary to create an encrypted tunnel with the associated remote access router. However, the authentication procedure presented in the paper is tedious and resource-consuming. Although the framework talks about protection of the confidentiality of exchanged information and the overall approach is analyzed, it has not

been tested in a detailed manner that could convince the readers about the efficiency of the approach in practical implementation cases.

The authors in [16] propose a framework of non-cooperative zero-sum game between genuine and malicious mesh routers and use mathematical tools and models for their approach. This game model solves the problem of grayhole attack where the malicious node drops a subset of packets that it receives. The game has a source node as the target and malicious node as the attacker; who compete with each other for limited resources and each node gains depending on the strategy of itself and that of the other. The attacker gains benefit from dropping packets and the target gains from forwarding packets successfully. Our approach adopts similar game theoretic model as a part of the total solution. However, the difference is that we circumvent the flaws of this paper's idea by using our own mathematical model and choosing appropriate parameter values. As an example, [16] takes 50% of the packet arrival rate to send buffer based on which the gains of both nodes vary. Therefore, it may be impractical because in reality, higher packet arrival rate is expected to minimize packet delay as well as large number of nodes should be involved in communications in any wireless mesh networks.

A novel algorithm named Channel-Aware Detection (CAD) has been adopted in the work presented in [17]. The authors in this paper use two different strategies to detect the grayhole attacks. Their approach detects a potential victim mesh node (i.e., which can be attacked) by hop-by-hop loss observation and traffic overhearing. A comparative performance analysis has been shown to detect and isolate the selective forwarding attackers [25] in multi-hop network scenario. The probability of miss detection or false alarm is analyzed and a design is proposed to limit these to certain threshold. However, the approach is complicated, focuses on narrow set of attacks, and is applicable only in some restrictive scenarios. This work basically focuses on the communication and signaling aspects in physical layer but is related to our work in the sense that some of the ideological concepts helped us in the formulation of our approach, which we will discuss later.

Several attentions have been devoted to investigate the use of cryptographic techniques to secure the information transmitted through the wireless network. Some other preliminary solutions have been addressed in ad hoc, sensor and wireless mesh networks to prevent different types of malicious attacks [18], [19], [20].

After presenting all these background knowledge, in the next section we present our proposed model.

2. Tackling Intruder with a Tricky Trap

It should be noted before further reading that our security model is for *intrusion tackling* or *intrusion handling*, instead of direct *intrusion detection* or *intrusion prevention* in WMN. The background knowledge noted so far could be useful while explaining our approach of handling the issue. We also clarify some terms in later sections to explain our position in better way and to differentiate among the terminologies.

The core concept of our approach is that; not always all the intruders in a network be harmful for the network. In fact, there are sometimes ways to get benefit out of it or utilizing it for the network's welfare or for its own benefit. Keeping this tricky fact in mind, we take a different approach to tackle an intrusion. Let us know about the assumptions before we proceed.

2.1. Considered Setting: Network Characteristics and Security Model

We assume a hybrid wireless mesh network where different types of devices could form the fringe part or could play the roles of mesh clients. A network model is shown in Figure 1. As it is understood from the figure, any node in the fringe parts could come and go, may be mobile, which allows a newcomer or even an *intruder* to try its luck in the network. We have noted before, even if a node within the legitimate mesh clients act as an attacker, in our case, we consider it as an intruder that is it has lost the legitimacy to stay in the network as a legal participant and is seen as a suspicious entity that has caused intrusion (illegitimate incursion) within the network perimeter. We assume that standard security components (i.e., cryptographic keys for data confidentiality, security measures, etc.) and other basic intrusion detection mechanisms are present within the network. The basic intrusion detection agents could be installed in any node in the network. Hence, our mechanisms start working after an intrusion is detected or some node is suspected of being an intruder. To capture the whole idea in a single sentence, "*We are interested to deal with the intruder if it is suspected to be such, after it has caused intrusion rather than purging it out directly from the network for its existence in the network*". By 'standard security components' we mean the cryptographic parameters, keys, and other security mechanisms that are used in a device that participates in a given network (The readers are suggested to go through the basic terms and preliminaries mentioned in Section 2 for a recap).

2.2. PaS Model: The Idea Behind

Once a node in the network is suspected as an intruder (by any of the standard components installed in the legitimate devices), our model is employed to force the intruder to work for the network. If it works for the network, we see little problem in allowing the node to stay in the network. That is because the routing packets and exchanged data within the network would be protected by other cryptographic measures in place as noted in the previous section. Instead of taking a straight negative decision to defuse it, we give it enough tasks to perform for forwarding any possible network packet to the next hops or to the intended destinations.

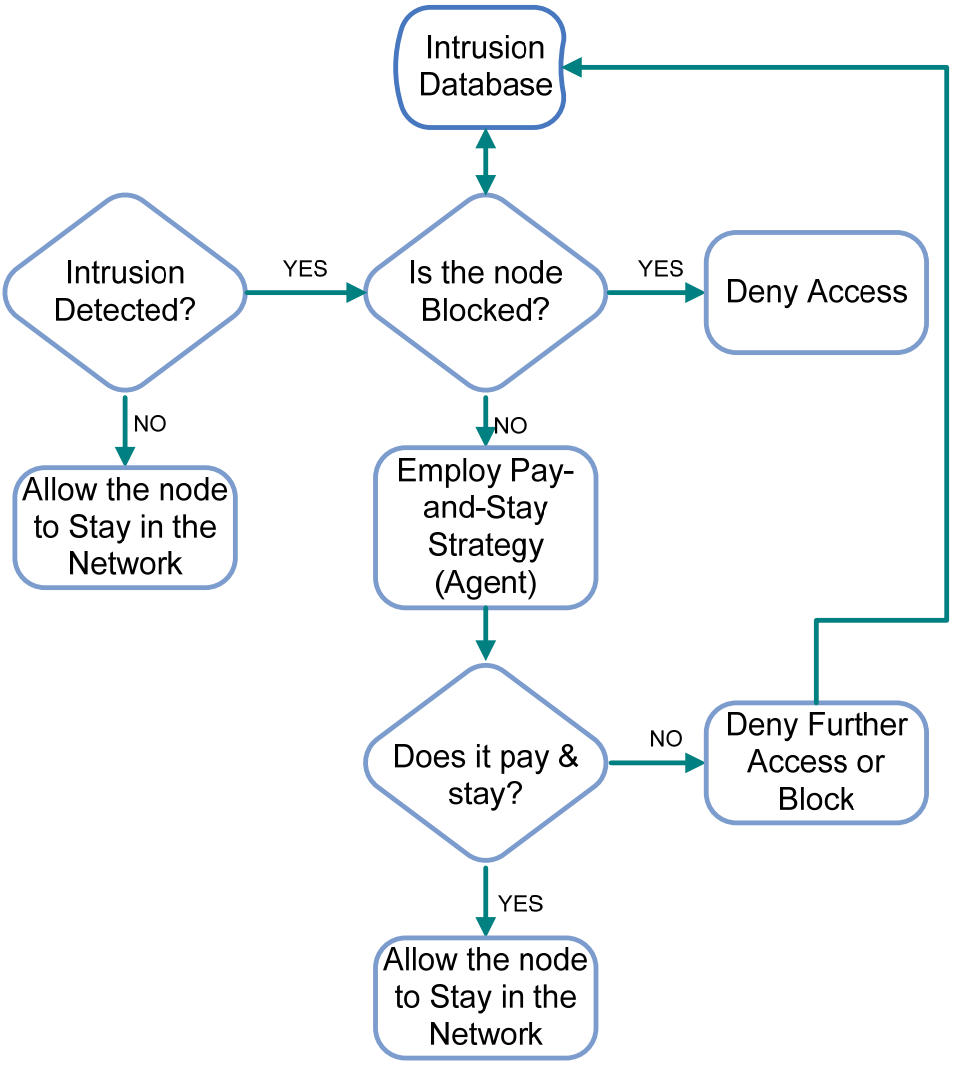

Figure 2. Operational diagram of our intrusion tackling model.

If the node is an intruder unwilling to participate in the forwarding process of the packets, we decide finally that the node is not suitable for staying in the network and must be purged out. Otherwise, by putting it in pressure to forward huge number of packets, we save network's other resources. Each forwarding takes energy for wireless transmission; hence, if an intruder happily does the network's legitimate nodes' job, we drain its energy or make it to pay for its survival/stay in the network. If the node drops the packets randomly or selectively, we catch this with our enforced mechanisms and mark it as a selective forwarder or we charge it for causing *selective forwarding*. To employ this policy, the intrusion tackling agent is installed on each legitimate mesh entity (mesh router or mesh clients).

Figure 2 shows an operational diagram of *PaS* intrusion tackling model. The intrusion database can be stored in any of the devices with good amount of storage space or could be partially maintained by each node that is, each node acts as the intruder tackler for its surrounding nodes. For primary intrusion detection, as noted earlier, any standard scheme could be utilized. Because of the structural dimension of WMN, such strategy is possible to use whereas for WSN or other wireless ad hoc networks, such strategy may not be used. As shown in the figure, our model gets activated after the IDS does its part; we deal with what to do *after* the intrusion, not *before* the intrusion. The core goal is to maximize or save the utilization of network resources by putting the burden of packet transmissions to a rogue entity. In case the rogue entity denies paying or giving the service, we purge it out from the network and thus this is an effort of delicately handling an intruder in a wireless mesh network setting.

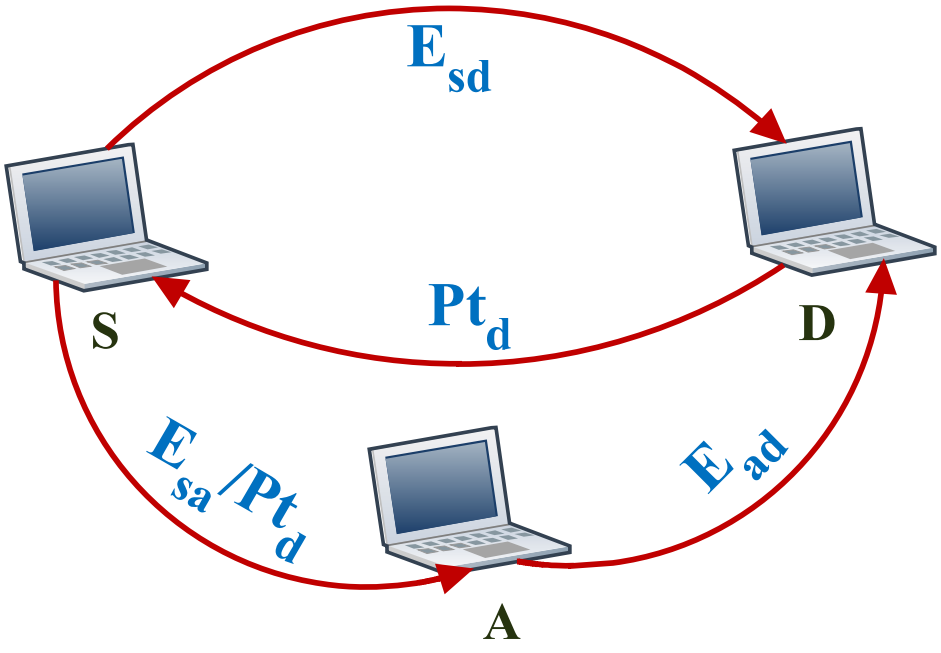

Figure 3. S sends packet directly and S sends packets via A.

The texts below explain how we achieve this PaS strategy for intrusion tackling. There are mainly two phases in our approach. The first phase is (i*) Game theory based PaS model*, and the second phase is (ii) *Marking the intruder and taking decision* (which is also the part of the intrusion tackling model). The following sub-sections illustrate our approach in detail.

2.3. Use of Game Theory to Put a Competition

Game theory [21] can be defined as the statistical model to analyze the interaction between a group of players, who act strategically. Figure 3 introduces a usual attack model where there are two players involved namely Player_1, which is the source node *S* and Player_2, which is the malicious/attacker (in our case, intruder) intermediate node *A*. Let *D* be the destination node and *N* be the finite set of all players. We limit our game to non-cooperative, incomplete information and zero-sum game model [22] where one player wins and the other player loses. Our target is that the intruder should spend more than the target to do any wrongdoing with the packet that it needs to forward to the destination. That means the intruder eventually has to pay heavily for its illegal staying within the network. It should be noted that we use the terms *intruder* and *attacker* interchangeably throughout the rest of the texts.

A. Mathematical model

Before presenting the mathematical model of our approach, in Table 1, we note down the critical notations used in this chapter for ease of reading and identification of various items at a glance.

Table 1. Basic notations and their meanings.

Notation	Meaning
$\boldsymbol{P_i}$	probability to defend the *i*th node in the network
$\boldsymbol{v_i}$	intermediate node
$\boldsymbol{v_{i-1}}$	upstream node
$\boldsymbol{v_{i+1}}$	downstream node
$\boldsymbol{\mu}$	packet arrival rate
$\boldsymbol{E_{sd}}$	energy spent for utility cost
$\boldsymbol{E_r}$	remaining energy
$\propto$	a constant
$\boldsymbol{p_a}$	probability of transmitting packets via Player_2
$\boldsymbol{p_d}$	probability of direct transmission of packets
$\boldsymbol{q_f}$	forwarding probability
$\boldsymbol{q_d}$	probability of dropping the packet
$\boldsymbol{Pt}$	points received

Let P_i be the probability to defend the *i*th node in the network. We assume that v_i is an intermediate node and v_{i-1} and v_{i+1} are the upstream and downstream nodes respectively. The total probability of defending all *N* nodes is, $\sum_{i=1}^{N} P_i$. The energy spent for utility cost is: $E_{sd} = \sum_{i=1}^{N} P_i$.

The remaining energy is: $E_r = 1 - \sum_{i=1}^{N} P_i$ where, $\sum_{i=1}^{N} P_i \leq 1$. Our objective is that the energy that needs to be spent by the intruder in order to cause trouble in packet flow or forwarding, must be more than the energy spent by the victim (which is sending or receiving the packets).

The energy of the sender to send via the attacker could be noted by the equation: $E_{sa} = \alpha \sum_{i=1}^{N} P_i$, where $\propto$ is a constant. The successful attack depends on the value of $\propto$. If $\propto > 1$, the attack succeeds. If $\propto = 1$, the energy spent by the attacker equals to that of the target. When $\propto = 0$, the attacker cannot attack, and $\propto < 1$ means that the attacker cannot drop any packet.

The state of the game is (m, n), where m is the sending buffer of Player_1 and n is the dropping buffer of Player_2. If one packet is present in the sending buffer of m of Player_1, then m will take a value of 1 and n can take value 0 or d, depending on whether any packet is dropped or not. We also denote μ as the probability that a new packet arrives at the sending buffer of Player_1. There are four possible states of the game and they are: $k_1 = (0,0), k_2 = (0, d), k_3 = (1,0), k_4 = (1, d)$. Therefore, the transition probabilities from one state to another state are calculated as follows:

When $(m = 1)$,

$$P_{(m,n)(m+i,n)}(x) = \begin{cases} (1-\mu)\left(p_d + p_a q_f\right) & ; if\ i = -1, n = 0 \\ (1-\mu)(p_a q_d) & ; if\ i = -1, n = d \\ \mu\left(p_d + p_a q_f\right) & ; if\ i = 0, n = 0 \\ \mu(p_a q_d) & ; if\ i = 0, n = d \end{cases} \quad (1)$$

When $(m = 0)$,

$$P_{(m,n)(m+i,n)}(x) = \begin{cases} (1-\mu) & ; \text{if i} = 0, \text{n} = 0 \\ (\mu) & ; \text{if i} = 1, \text{n} = \text{d} \end{cases} \quad (2)$$

where, μ is the arrival rate of packets in the send buffer and *x* is the joint strategy.

For example, assume that the current state of system is $(1,0)$. Player_1 (i.e, *S*) has packet in its send buffer. It uses two strategies: transmit packet directly or transmit via *A*. If *S* transmits packet directly to *D*, then the states are $(0,0)$ or $(1,0)$ with probability p_d. Otherwise, it transmits packets via Player_2 (i.e., *A*) with probability, p_a. A either drops the packet or forwards it to D. If it drops, then the states become $(0,d)$ or $(1,d)$. If *A* forwards the packet, then the next states will be $(0,0)$ or $(1,0)$. Note that *A* is the potential intruder in this case.

The strategy set for Player_1 is $S_1 = \{s_1, s_2\}$, meaning that Player_1 forwards the packet either directly to destination D (s_1) or via A (s_2). Mixed strategies (denoted as *x*) that correspond to S_1 are $\pi_s(s_1, s_2) = (p_d, p_a)$, where $p_d + p_a = 1$. The strategy set of Player 2 is $A_2 = (a_1, a_2)$. Mixed strategies corresponding to the action of A_2 are $\pi_a(a_1, a_2) = (q_f, q_d)$ where, $q_f + q_d = 1$. Here, q_d = probability of dropping the packet. Hence, $(\pi_s, \pi_a) = (p_d, p_a, q_f, q_d)$.

The destination *D* gives some points to source *S* for the transmitted packet. When the source node *S* sends the packet through the path *S*→*D*, node *S* receives some points of Pt_d from D. When *S* transmits packets via *A*, it receives points of Pt_d from *D* and it gives *A* some points, Pt_{sa}. . If *S* does not receive any point from *D* for the transmitted packet, it means that the packet did not reach to *D* successfully. Each packet transmission from v_i node to v_{i+1} node causes an energy spending Ev_iv_{i+1} . Therefore, depending on the energy spent and points received by the source and attacker, the nodes *S* and *A* will remain with the following net utility:

$$U_s = \begin{cases} Pt_d - E_{sd}\ ; & S\ transmits\ directly\ to\ D. \\ Pt_d - Pt_{sa} - E_{sa}\ ; & S\ transmits\ to\ D\ via\ A. \\ -Pt_{sa} - E_{sa}\ ; & node\ A\ drops\ the\ packet. \end{cases} \quad (3)$$

If $(-Pt_{sa} - E_{sa}) < (Pt_d - E_{sd}) < (Pt_d - Pt_{sa} - E_{sa})$, the utility of *S* will decrease if *A* drops the packet compared to the utility it receives when a packet reaches *D*.

$$U_a = \begin{cases} Pt_{sa} - E_{ad}\ ; A\ forwards\ the\ packet\ to\ D. \\ Pt_{sa} + \beta\ ; \quad node\ A\ drops\ the\ packet. \end{cases} \quad (4)$$

where β is the profit earned by node A. If $(Pt_{sa} - E_{ad}) < (Pt_{sa} + \beta)$, the utility earned from dropping the packet is higher than the utility received from *S* for transmitting the packet. However, the utility can be calculated from the equations below based on the probability of dropping and forwarding the packets.

$$U_s(x) = \mu(1-\mu \times p_a q_d)\{p_d(Pt_d - E_{sd}) + p_a(q_f(Pt_d - Pt_{sa} - E_{sa}) + q_d(-Pt_{sa} - E_{sa}))\} + \mu^2 \times p_a q_d\{p_d(Pt_d - E_{sa}) + p_a(q_f(Pt_d - pt_{sa} - E_{sa})) + p_a(q_d(-Pt_{sa} - E_{sa}))\} \quad (5)$$

And,

$$U_a(x) = \mu(1-\mu \times p_a q_d)\{p_a\big(q_f(Pt_{sa} - E_{ad}) + q_d(Pt_{sa} + \beta)\big)\} + \mu^2 \times p_a q_d\{p_a(q_f(Pt_{sa} - E_{ad}))\} + \mu^2 \times p_a q_d(p_a q_d(Pt_{sa} + \beta)) \quad (6)$$

B. Marking the Intruder and Taking Decision

In this section, we describe a Multi-hop Acknowledgement Based algorithm to detect malicious node(s) doing selective forwarding attack. Because of the structure of WMN, this method is possible to be utilized. We know that selective forwarding attack is one of the most dangerous attacks because the packets are dropped randomly which may contain sensitive data. In this algorithm, multiple nodes need to be selected as acknowledgement points in WMNs. This means that those mesh nodes are responsible for sending an ACK packet after receiving a packet from a source node or nearest intermediate source nodes. We assume that the WMNs are operating under an ideal channel quality and majority of the mesh routers are normal-behaving. We are considering that the packet loss appears only due to malicious activity from an intruder. Moreover, since there may be multiple existing routes from a source mesh node to a destination mesh node and a source node may receive multiple route replies of each of its route requests, we encourage the source node to keep record of each route for future references. It should be noted here that dealing with physical layer or channel-level matters are out of the scope of this work as we focus on the theoretical framework and mathematical model of the operational concept.

In Figure 4, we show the structure of a wireless mesh network where *S* is the source node and *D* the destination node. We assume *N* is the total number of mesh nodes in the forwarding path. *M* is the number of malicious nodes among *N*. Let *X* be the normal-behaving nodes between each two malicious nodes and *Y* be the number of acknowledgement points in the forwarding path. We consider *Z* as the percentage of randomly selected check points.

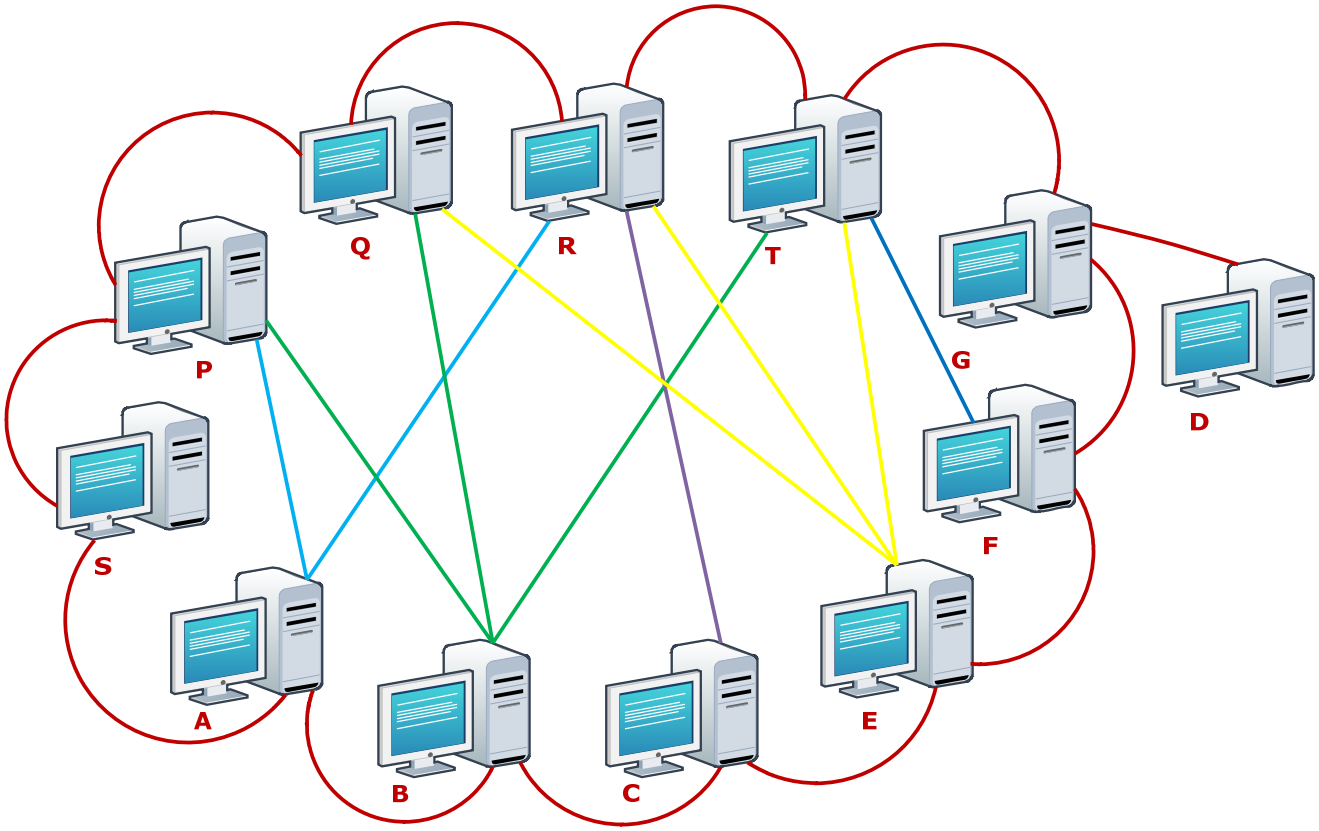

Figure 4. Multi-hop acknowledgement.

When the source node S sends a route request, it receives several route replies. Let us consider that *S* chooses the route SABCEFG→D, where *E* is the malicious node. We are considering two selected acknowledgement points (i.e., Y=2) namely *B* and *F*. *B* and *F* will acknowledge back after they receive the packets from the source mesh nodes. Therefore, the following possibilities may occur if:

Scenario 1: One of the nodes is malicious in the forwarding path.
Scenario 2: One or more nodes are malicious in the forwarding path.
Scenario 3: Both the Acknowledgement points B and F are malicious
Scenario 4: Either B or F is malicious.

This algorithm uses two approaches: hop-by-hop loss observation and traffic overhearing to detect malicious node on the path of data flow. More specifically, we assume v_i as an intermediate node and v_{i-1} and v_{i+1} as the upstream and downstream node respectively. v_{i+1} receives a packet from v_{i-1}, then it updates itself with the packet count history and with the corresponding packet sequence number and

then buffers the link layer acknowledgment (ACKs) that it receives for each packet and then forwards it to v_{i-1} (i.e., downstream node). We denote w_s as the total number of packets that are successfully sent-received by the source S to destination D. $n_{v_i \to v_{i+1}}$ is the number of packets received successfully by v_{i+1} (i.e., this is the number of successfully received packets from any intermediate node to its downstream node).

Two operations are performed when the mesh router forwards a packet to the downstream node as explained in this paragraph. When each packet is relayed to the downstream traffic, the mesh router or upstream node buffers the ACKs and overhears the downstream traffic to check whether it (downstream node) forwarded or tampered the packet. The upstream node observes these two operations and then makes a simple analysis of the scenario.

The downstream node maintains two parameters. They are; (a) probability of acknowledgment (ACK) which we denote as P_{Ack} and (b) probability of no-acknowledgment (NACK), P_{NAck}. Probability of ACK (P_{Ack}) is computed as $P_{Ack} = 1 - P_{NAck}$ and the probability of no-acknowledgment is computed as $P_{NAck} = (n_t + n_d)/n_f$, where n_t is the number of tampered packets, n_d is the number of dropped packets, and n_f is the number of total forwarded packets.

We introduce two packets: PROBE packet and PROBE_ACK to detect the malicious routers. The PROBE packet is used by the source node *S* with every w_s data packets to the destination node *D*. When the source node *S* sends the PROBE packet through the path, each node in the path marks the PROBE packet with the detection parameters and this is termed *packet marking*. A PROBE packet sent to destination by the source node is also marked by it (i.e., *S*) with the number of packets that will be transmitted to a particular destination node. When the PROBE packet is passed along the path, each node v_i attaches a mark of its opinion to the downstream node (v_{i+1}). The opinion is calculated by observing the downstream node's behavior by the transmitter node. The opinion of downstream node is calculated as follows:

- If ($P_{NAck} > t_m$), it means malicious behavior.
- If ($P_{NAck} < t_m$), it means normal behavior.

where t_m is the monitoring threshold and it carries values between 0 and 1. As the PROBE packet is passed through the path, the node also appends the behavior parameter to the PROBE packet. The behavior parameter represents the observation of node v_{i+1} about the behavior of the upstream node, v_i.

The behaviour of the node is calculated by determining the loss rate of the packets over the link v_i to v_{i+1} . It is calculated by the following formulae:

- If $(L_{v_i \to v_{i+1}} > t_l)$, malicious behavior is detected.
- If $(L_{v_i \to v_{i+1}} < t_l)$, normal behavior.

where, $(L_{v_i \to v_{i+1}} = 1 - (n_{v_i \to v_{i+1}} / n_{v_{i-1} \to v_i}))$ is the loss rate of the link that is observed by the node, v_{i+1} . t_l is the loss rate threshold that can take any value between 0 and 1. The algorithm will detect the malicious behavior with higher probability with the lower values of t_l and t_m.

3. Analysis of Our Approach

3.1. Experimental Results

For the game theoretic model analysis, we substititute the values for required energy to transmit packets from S to D either directly or via A and the points earned by source S and A as follows: $E_{sd} = 0.6$, $E_{sa} = E_{ad} = 0.05$, $Pt_d = 1$, $Pt_{sa} = 0.3$. We assume that the packet arrival rate μ to send buffer is quite fast; $\mu = 0.8$, and $\beta = 0.2$.

Using equation (5) and (6), we obtained the utitilty of Player 1 and Player 2. We represented Figures (5 to 9) of utility of *S* and *A* as a function of drop probability using MATLAB. The packet dropping probabilitiy is chosen between 0 and 1. It is observable from the Figures (5 to 9) that the utility of *S* is decreasing and utility of *A* is increasing with the increase of dropping probability.

Player 2 reaches the maximum utility when source *S* transfers all the packets via *A* with the highest dropping probability. It can be seen from Figure 9 where $p_a = 1$ and $q_d = 1$, the maximum utility of $U_a = 0.4$. On the other hand, for $q_d = 1$, Player 1 has its maximum utility $U_s = 0.256$, when the probability of sending packets direcly to *D* increases. The maximum utility of *S* is shown in Figure 5 where $p_d = 0.8$ and $q_d = 0.1$. Figures 10 to 14 represent the utility of *S* and *A* as a function of forward probability to *A*, p_a. The forward probability is chosen between 0 and 1.

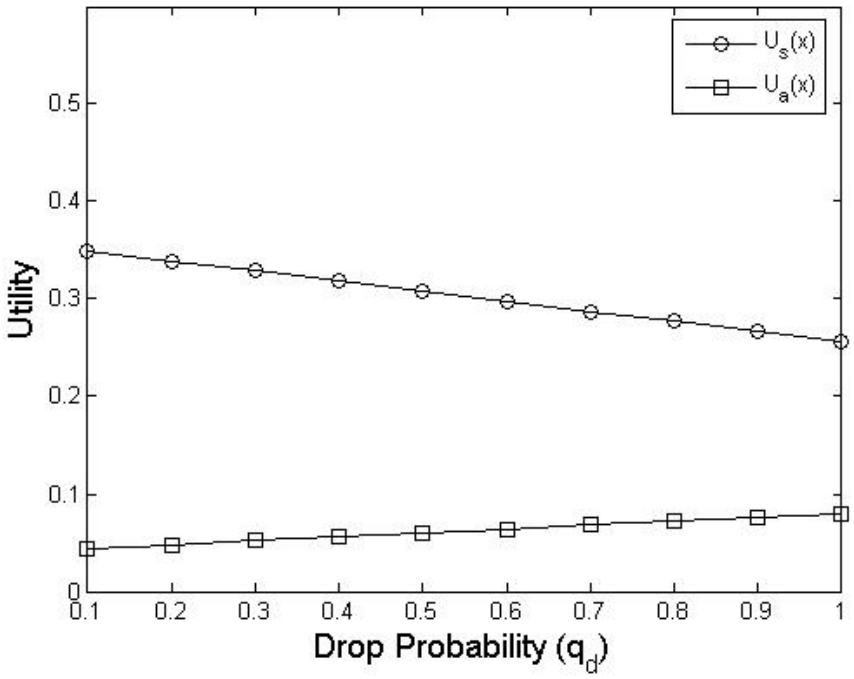

Figure 5. Increasing the utilities of A and decreasing the utilities of S with respect to different drop probabilities of q_d when $p_d = 0.8$ and $p_a = 0.2$.

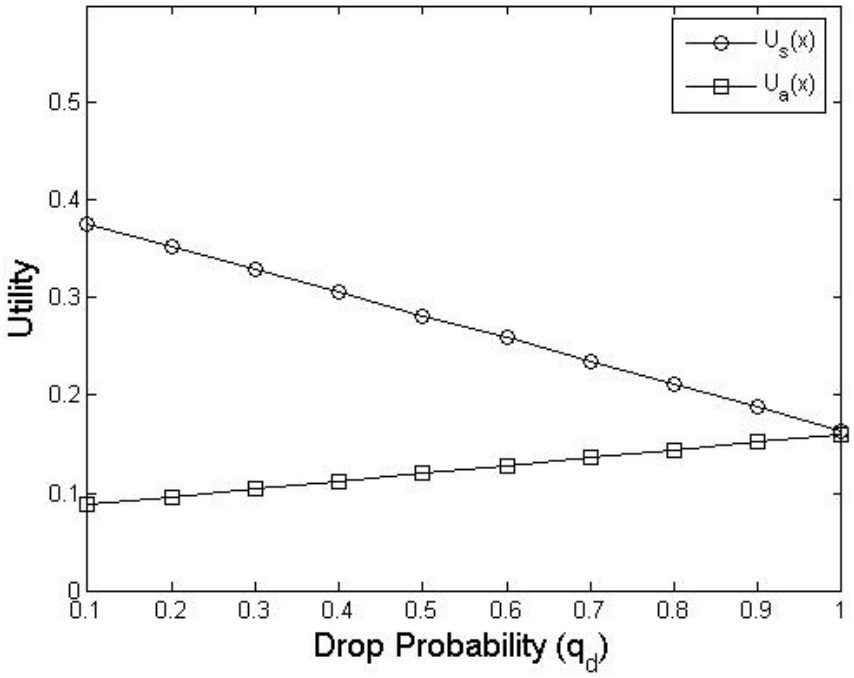

Figure 6. Increasing the utilities of A and decreasing the utilities of S with respect to different drop probabilities of q_d when $p_d = 0.6$ and $p_a = 0.4$.

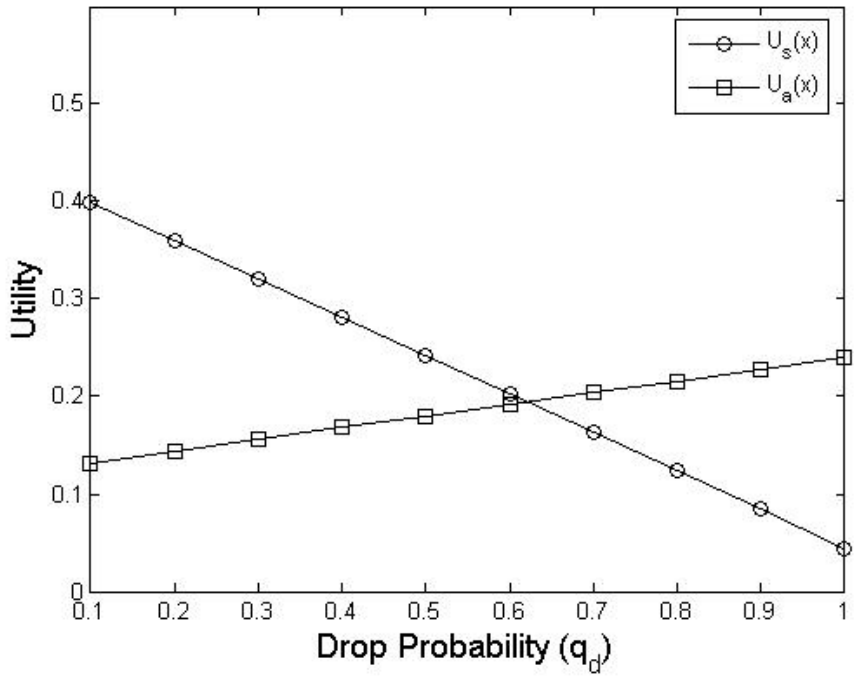

Figure 7. Increasing the utilities of A and decreasing the utilities of S with respect to different drop probabilities of q_d when $p_d = 0.4$ and $p_a = 0.6$.

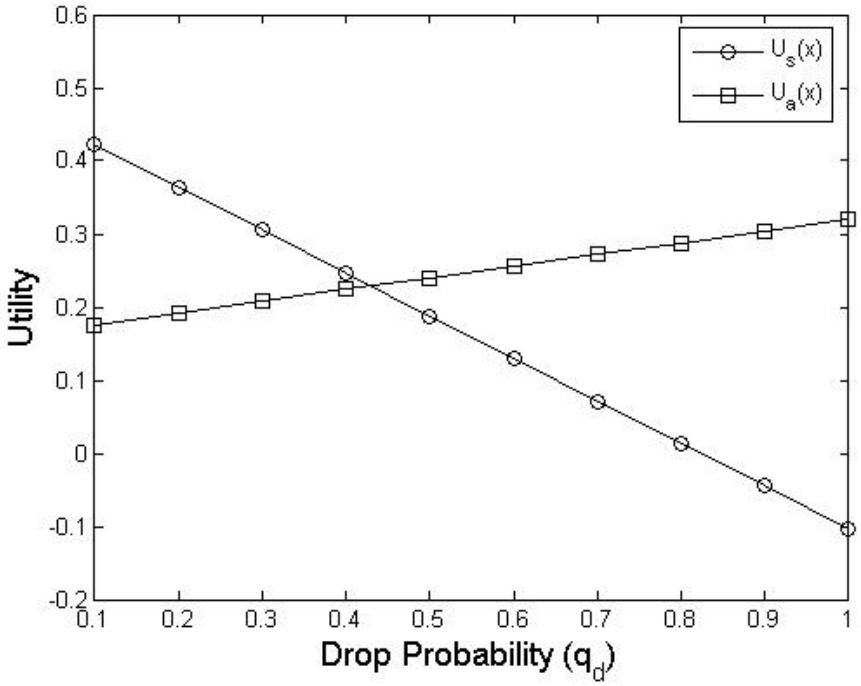

Figure 8. Increasing the utilities of A and decreasing the utilities of S with respect to different drop probabilities of q_d when $p_d = 0.2$ and $p_a = 0.8$.

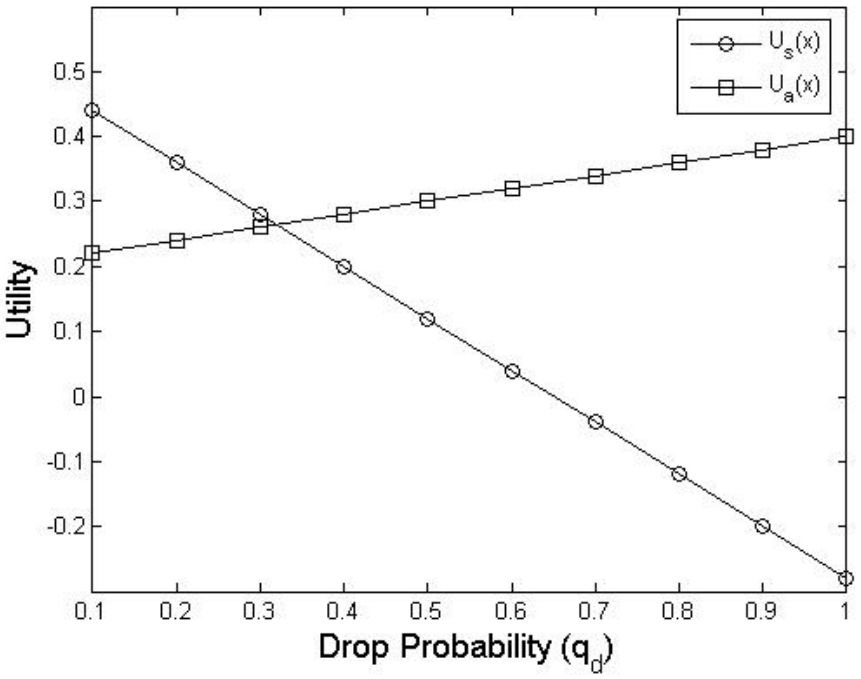

Figure 9. Increasing the utilities of A and decreasing the utilities of S with respect to different drop probabilities of q_d When, $p_d = 0$ and $p_a = 1$.

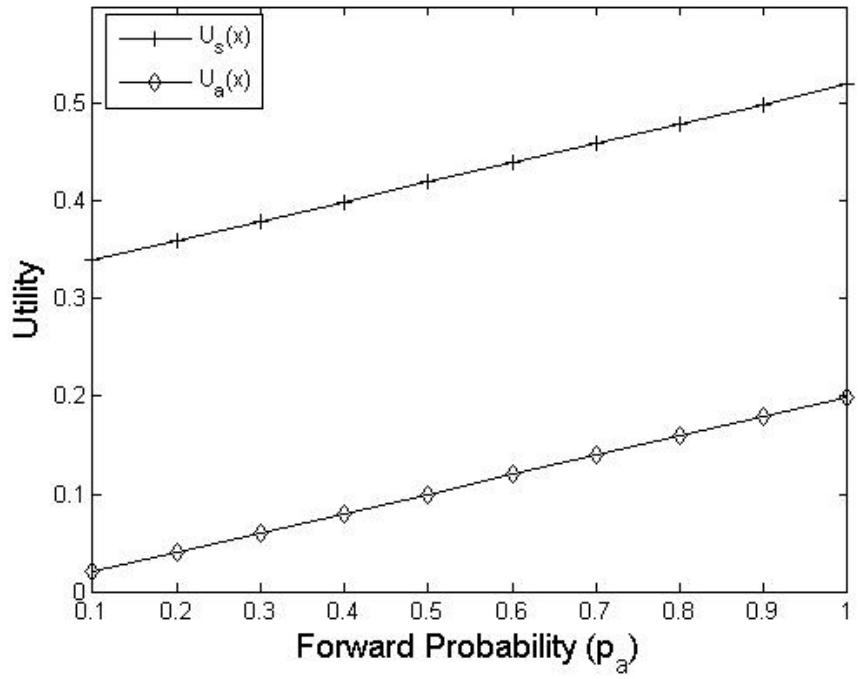

Figure 10. The increase of utility S and A as a function of p_b with respect to $q_f = 1$ and $q_d = 0$.

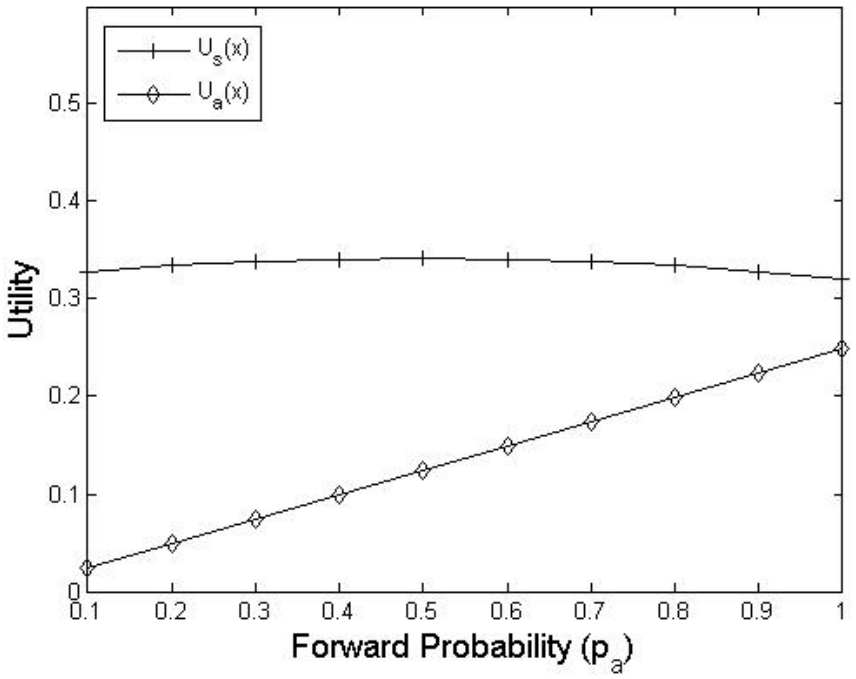

Figure 11. The increase of utilities S and A as a function of p_b with respect to $q_f = 0.75$ and $q_d = 0.25$.

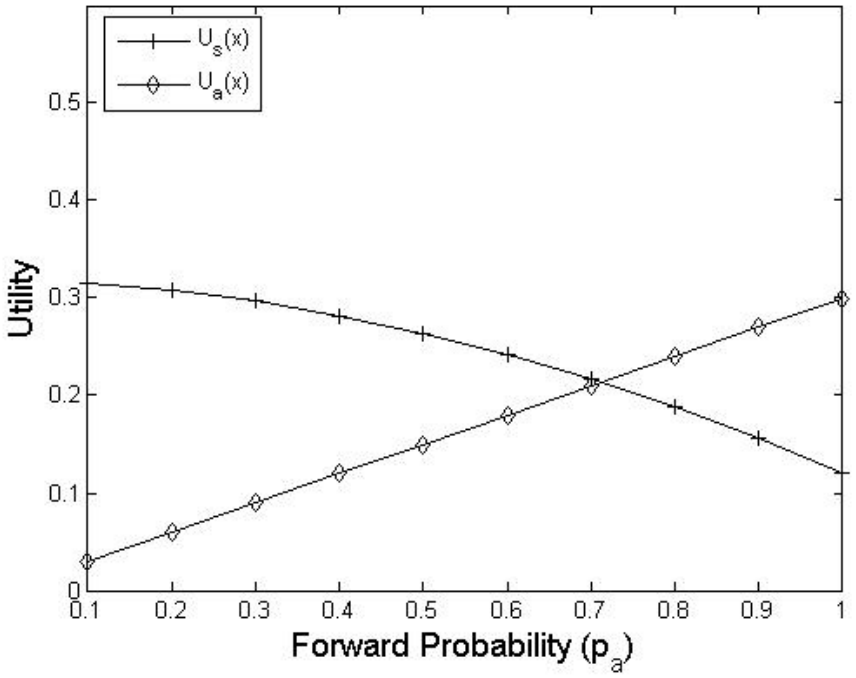

Figure 12. The increase of utility A and decrease of utility S as a function of p_b with respect to $q_f = 0.5$ and $q_d = 0.5$.

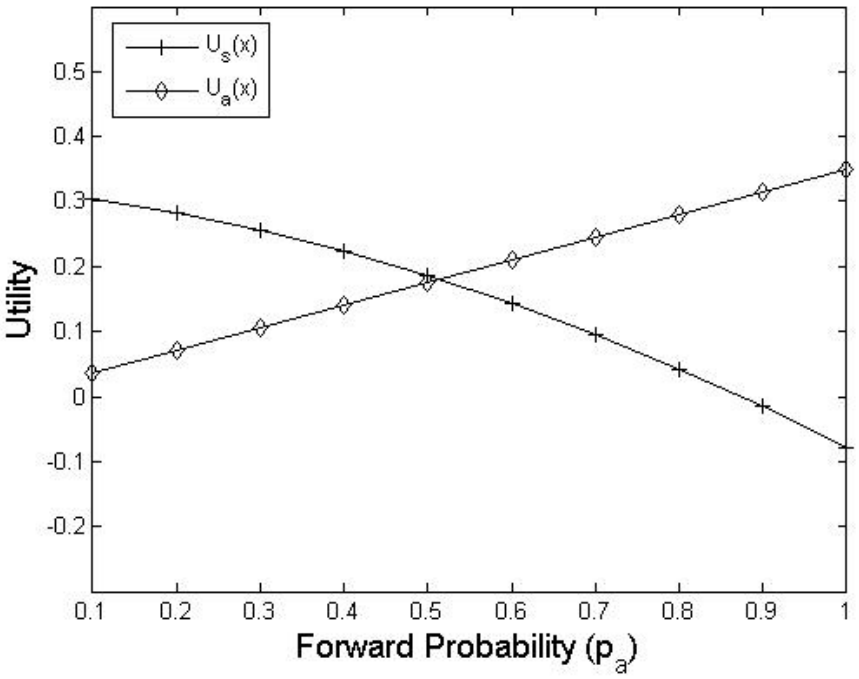

Figure 13. The increase of utility A and decrease of utility S as a function of p_b with respect to $q_f = 0.25$ and $q_d = .75$.

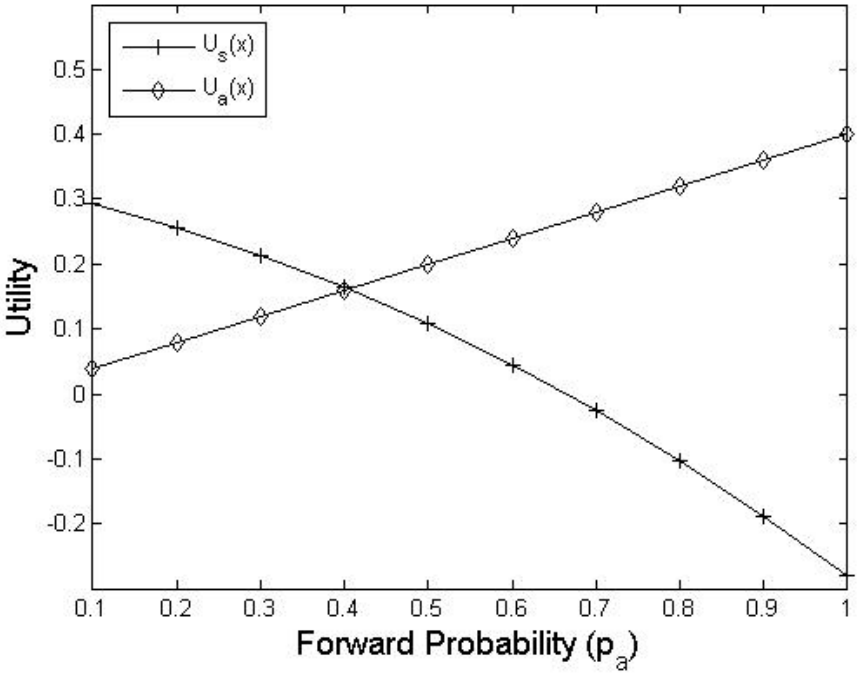

Figure 14. The increase of utility A and decrease of S as a function of p_b with respect to $q_f = 0$ and $q_d = 1$.

The forward probabilities are $q_f = 1$ and $q_f = 0.75$ and the drop probabilities are $q_d = 0$ and $q_d = 0.25$ in the Figure 10 and Figure 11. It is clear that in Figure 10, the utilities of *S* and *A* are increasing. The maximum utility of *S* is 0.5 and the maximum utility of *A* is 0.2. In Figures (11, 12, 13, 14), the utility of S is overall decreasing (with a slight bent increase and going down in Figure 11) and the utility of *A* is increasing and the maximum utility of A is 0.4 ; the forward probabilities are, $q_f = 0.75$, $q_f = 0.5$, $q_f = 0.25$, and $q_f = 0$ and the drop probabilities are $q_d = 0.25$, $q_d = 0.5$, $q_d = 0.75$, and $q_d = 1$.

3.2. Marking the Intruder Considering Various Cases

In the malicious behavior detection phase, the following possible cases may occur when the upstream and downstream nodes are combined to detect malicious activities:

Case 1: If $P_{NAck_{v_i \to v_{i-1}}} > t_m$ and $L_{v_i \to v_{i+1}} > t_l$.

The node v_i either drops or tampers the packets. The probability of NACK is greater than the monitoring threshold, t_m. The node v_{i-1} , the upstream node will observe node v_i on whether it drops the packets or tampers it. Node v_{i-1} will increase n_d which is the number of dropped packets and also n_t which is the number of tampered packets. The downstream node, v_{i+1} will observe if loss rate is greater than the threshold t_l, loss rate threshold. The upstream and downstream will observe if node v_i is misbehaving.

Case 2: If $P_{NAck_{v_i \to v_{i-1}}} < t_m$ and $L_{v_i \to v_{i+1}} > t_l$.

In this case, the monitoring threshold is greater than the probability of NACK from node v_{i-1} to v_i. The node v_i is behaving normally. If the observed loss rate of link from v_i to v_{i+1} is greater than the loss rate threshold, node v_i is misbehaving. According to the upstream node, node v_i is normal but on the other hand the downstream node can detect if node v_i is misbehaving. To overcome this problem, we need to verify link layer acknowledgments that is received by the upstream node v_{i-1} for each packet that is forwarded successfully by the node, v_i .

Case 3: If $P_{NAck_{v_i \to v_{i-1}}} > t_m$ and $L_{v_i \to v_{i+1}} < t_l$.

In this case, the upstream node v_{i-1} has a greater probability of NACK and is greater than the monitoring threshold, t_m . In this case, there is a misbehaving activity at the node v_i . On the other hand, the observed loss rate link from v_i to v_{i+1} is lower than t_l, which is the loss rate threshold. According to upstream node v_{i-1} , the node v_i is misbehaving and downstream node will consider node v_i as normal.

To overcome this issue, the upstream node can detect the misbehaving node v_i by observing false information in the PROBE packet.

Case 4: If $P_{NAck_{v_i \to v_{i-1}}} < t_m$ and $L_{v_i \to v_{i+1}} < t_l$.
The downstream and the upstream nodes do not detect any misbehaving node.

4. Applicability and Future Network Vision

Our intrusion tackling model is designed for protecting the network from a wide range of security attacks that target the routing mechanisms of the network. The basic IDS mechanisms employed on the devices could notify a suspected intruder and when our model gets activated to handle the case, we ensure the proficiency in dealing with it to use the apparent negative entity for positive purpose. Only when it is proven to be a serious threat for the network, we retract its permit to participate in the network. The preliminary IDS mechanism acts as the primary defense against intrusion activity and our mechanism acts as the final line of defense against malicious intrusion. The behavioral analysis, to mark the intruder, sets the solid defense strategy to make our model effective in practical scenarios. Because of the features of WMN with the required amount of resources, this model works fine and proves to be effective while for other wireless networks like WSN (wireless sensor network), MANET (Mobile ad hoc network), and VANET (Vehicular ad hoc network), this model is not directly applicable.

From the higher level view however, all the above mentioned wireless technologies fall under the category of wireless self-organizing networks or ad hoc networks. Hence, putting all of them under an umbrella term, we could fit them in various future networking technologies like pervasive or ubiquitous computing, Internet of Things (IoT), Future Internet, Cloud computing, and so on [24]. It is expected that WMN, as a wireless network technology will blend well within these emerging technologies and concepts. If it is so, then, the basic principle of the *PaS* model could be applied in various scenarios. Even if the exact model may not be applied, it is possible to think of giving the intruder some waiver to stay in any of the future networks so that when it does more good than evil, the network in an intelligent manner utilizes its capacities rather than alienating it without giving some chance. In fact, a concept like pervasive computing would allow thousands of computation enabled devices to work together in a blended environment where it would be extremely difficult to mark any entity as a clear intruder or unwanted node. This is because; all those good and bad entities together would form a pervasive or ubiquitous environment with a complete mixture of human life and various device technologies. Likewise, other

future or next-generation computing and network technologies will have various applicable scenarios considering *PaS* model's core idea.

5. Wireless IDPS: The Features and Differences to Know

IDPS (Intrusion Detection and Prevention System) is basically the combination of detection and prevention mechanisms [26]. Before we put an end to this chapter, we feel that it is necessary for the readers to have some idea about various IDPS technologies commonly used for wireless networking. As our mechanism does not fall under any clear category, we referred to our approach as '*intruder tackling*' because we let the intruder stay in the network even after finding it out, which is conflicting to any IDS, IPS, or IDPS's main objective. The idea behind putting this section here is to make further clarification of these terminologies so that the readers could be able to make proper distinctions among these mechanisms.

A wireless IDPS monitors wireless network traffic and analyzes wireless networking protocols to identify malicious behavior. However, it cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring. It is most commonly deployed within the range of an organization's wireless network to monitor it, but it can also be deployed to locations where unauthorized wireless networking could be occurring.

Because of the transmission methods, wireless network attacks differ from those on wired networks. However, the basic components involved in a wireless IDPS are the same as the network-based IDPS: consoles, database servers, management servers and sensors. A wireless IDPS monitors the network by sampling the traffic. There are two frequency bands to monitor (2.4 GHz and 5 GHz), and each band includes many channels. A sensor (here, we mean, any kind of sensing mechanism) is used to monitor a channel at a time and it can switch to other channels as needed.

We should mention that most of the WLANs (Wireless LANs) use the Institute of Electrical and Electronics Engineers (IEEE) 802.11 family of WLAN standards [24]. IEEE 802.11 WLANs have two main architectural components:

- A station, which is a wireless end-point device (e.g., laptop computer, personal digital assistant).
- An access point, which logically connects stations with an organization's wired network infrastructure or other network.

Some WLANs also use wireless switches, which act as intermediaries between access points and the wired network. A network based on stations and access points is configured in infrastructure mode; a network that does not use an access point, in which stations connect directly to each other, is configured in ad hoc mode. Nearly all organizational WLANs use infrastructure mode. Each access point in a WLAN has a name assigned to it called a service set identifier (SSID). The SSID allows stations to distinguish one WLAN from another.

Wireless sensors have several available forms. A dedicated sensor is usually passive, performing wireless IDPS functions but not passing traffic from source to destination. Dedicated sensors may be designed for fixed or mobile deployment, with mobile sensors used primarily for auditing and incident handling purposes (e.g., to locate rogue wireless devices). Sensor software is also available bundled with access points and wireless switches. Some vendors also have host-based wireless IDPS sensor software that can be installed on stations, such as laptops. The sensor software detects station misconfigurations and attacks within range of the stations. The sensor software may also be able to enforce security policies on the stations, such as limiting access to wireless interfaces.

If an organization uses WLANs, it most often deploys wireless sensors to monitor the radiofrequency range of the organization's WLANs, which often includes mobile components such as laptops and personal digital assistants. Many organizations also use sensors to monitor areas of their facilities where there should be no WLAN activity, as well as channels and bands that the organization's WLANs should not use, as a way of detecting rogue devices.

5.1. Wireless IDPS Security Capabilities

The main advantages of Wireless IDPSs include detection of attacks, misconfigurations, and policy violations at the WLAN protocol level, primarily examining IEEE 802.11 protocol communication. The major limitation of a Wireless IDPS is that it does not examine communications at higher levels (e.g., IP addresses, application payloads). Some products perform only simple signature-based detection, whereas others use a combination of signature-based, anomaly based, and stateful protocol analysis detection techniques. Most of the types of events commonly detected by wireless IDPS sensors include unauthorized WLANs and WLAN devices and poorly secured WLAN devices (e.g., misconfigured WLAN settings). Additionally, the Wireless IDPSs can detect unusual WLAN usage patterns, which could indicate a device compromise or unauthorized use of the WLAN, and the use of wireless network

scanners. Other types of attacks such as Denial of Service (DoS) conditions, including logical attacks (e.g., overloading access points with large numbers of messages) and physical attacks (e.g., emitting electromagnetic energy on the WLAN's frequencies to make the WLAN unusable), can also be detected by wireless IDPSs. Some wireless IDPSs can also detect a WLAN device that attempts to spoof the identity of another device.

Another significant advantage is that most wireless IDPS sensors can identify the physical location of a wireless device by using triangulation – estimating the device's approximate distance from multiple sensors from the strength of the device's signal received by each sensor, then calculating the physical location at which the device would be, the estimated distance from each sensor. Handheld IDPS sensors can also be used to pinpoint a device's location, particularly if fixed sensors do not offer triangulation capabilities or if the device is moving.

Wireless IDPS overcome the other types of IDPS by providing more accurate prevention; this is largely due to its narrow focus. Anomaly-based detection methods often generate high false positives, especially if threshold values are not properly maintained. Although many alerts based on benign activities might occur, such as another organization's WLAN being within range of the organization's WLANs, these alerts are not truly false positives because they are accurately detecting an unknown WLAN.

Some tuning and customization are required for the Wireless IDPS technologies to improve their detection accuracy. The main effort required in the Wireless IDPS is in specifying which WLANs, access points, and stations are authorized, and in entering the policy characteristics into the wireless IDPS software. As wireless IDPSs only examine wireless network protocols, not the higher-level protocols (e.g., applications), generally there is not a large number of alert types, and consequently not many customizations or tunings that are available.

Wireless IDPS sensors provide two types of intrusion prevention capabilities:

- Some sensors can terminate connections through the air, typically by sending messages to the end points telling them to dissociate the current session and then refusing to permit a new connection to be established.
- Another prevention method is for a sensor to instruct a switch on the wired network to block network activity involving a particular device on the basis of the device's media access control (MAC) address or switch port. However, this technique is only effective for blocking the device's communications on the wired network, not the wireless

network.

An important consideration when choosing prevention capabilities is the effect that prevention actions can have on sensor monitoring. For example, if a sensor is transmitting signals to terminate connections, it may not be able to perform channel scanning to monitor other communications until it has completed the prevention action. To mitigate this, some sensors have two radios – one for monitoring and detection, and another for performing prevention actions.

5.2. Wireless IDPS Limitations

The wireless IDPSs offer great detection capabilities against authorized activities, but there are some significant limitations. The use of evasion techniques is considered as one of the limitations of some wireless IDPS sensors, particularly against sensor channel scanning schemes. One example is performing attacks in very short bursts on channels that are not currently being monitored. An attacker could also launch attacks on two channels at the same time. If the sensor detects the first attack, it cannot detect the second attack unless it scans away from the channel of the first attack.

Wireless IDPS sensors (physical devices) are also vulnerable to attack. The same denial of service (DoS) attacks (both logical and physical) that attempt to disrupt WLANs, can also disrupt sensor functions. Additionally, sensors are often particularly vulnerable to physical attacks because they are usually located in hallways, conference rooms, and other open areas. Some sensors have anti-tamper features, which is designed to look like fire alarms that can reduce the possibility of physically being attacked. All sensors are vulnerable to physical attacks such as jamming that disrupts radio-frequency transmissions; there is no defense against such attacks other than to establish a physical perimeter around the facility so that the attackers cannot get close enough to the WLAN to jam it.

We should mention that the wireless IDPSs cannot detect certain types of attacks against wireless networks. An attacker can passively monitor wireless traffic, which is not detectable by wireless IDPSs. If weak security methods are used, for example, Wired Equivalent Privacy (WEP), the attacker can then perform off-line processing of the collected traffic to find the encryption key used to provide security for the wireless traffic. With this key the attacker can decrypt the traffic that was already collected, as well as any other traffic collected from the same WLAN. As the Wireless IDPSs cannot detect certain types of attacks against wireless networks, it cannot fully compensate for the use of insecure wireless networking protocols.

We hope that from this discussion, it is clear that there are some basic differences between the IDPS technologies of general wireless networking and that of the Wireless Mesh Network.

6. Potential Research Fields and Concluding Remarks

This chapter's main focus was to present an intrusion tackling model for wireless mesh networks with the idea of utilizing the resources of an intruder before taking final decision of removing it from the network. This approach proves to be useful for WMN and other schemes dealing with intrusion detection or intrusion prevention could be employed side-by-side. In that case, better protection could be achieved to limit the number of false positives. Also, if applied as the only intrusion tackling module, other security schemes dealing with various types of attacks could work well alongside this mechanism. If the intruders' resources are used for the network and strong cryptographic mechanisms protect the network packets, this model can prove to be one of the best solutions to deal with WMN intrusion. As future works, the idea could be extended to find out more efficient solution to tackle huge number of colluding intruders who might make packet drop seemingly a natural event. As none of the previous works dealt with intrusion in this way, this work opens a new frontier to the researchers to work on intrusion tackling rather than direct exclusion by detection or prevention. New models could be developed in this area and numerous ways could be thought of based on the findings presented in this work.

7. Acknowledgments

This work was supported by Networking and Distributed Computing Laboratory (NDC Lab), KICT, IIUM. Al-Sakib Khan Pathan is the corresponding author.

8. References

[1] Pathan, A.-S.K. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET. ISBN: 978-1-4398-1919-7, Auerbach Publications, CRC Press, Taylor & Francis Group, USA, 2010.

[2] Bruno, R., Conti, M. and Gregori, E., "Mesh Networks: Commodity Multihop Ad Hoc Networks", IEEE Communications Magazine, Volume 43, Issue 3, 2005, pp. 123–131.

[3] Shila D.M. and Anjali, T., "Defending Selective Forwarding Attacks in WMNs", IEEE International Conference on Electro/Information Technology 2008 (EIT'08), Iowa, USA, May 18-20, 2008, pp. 96-101.

[4] Wireless Mesh Networks and Applications in the Alarm Industry. WhitePaper, AES Corporation, 2007, available at: http://www.aes-intellinet.com/documents/AESINT-WhitePaper.pdf (last accessed January 09, 2012)

[5] Akyildiz, I.F. and Wang, X., “A survey on wireless mesh networks”, IEEE Communications Magazine, Volume: 43, Issue: 9, 2005, pp. S23-S30.

[6] Deng, H., Li, W., and Agrawal, D.P., “Routing Security in Wireless Ad Hoc Networks”, IEEE Communication Magazine, Volume: 40, Issue: 10, October, 2002, pp. 70-75.

[7] Zhang, Z., Nait-Abdesselam, F., Ho, P.-H., and Lin, X., "RADAR: a ReputAtion-based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks", IEEE Wireless Communications and Networking Conference, 2008 (WCNC 2008), Las Vegas, NV, USA, pp. 2621-2626.

[8] Li, H., Xu, M., and Li, Y., "The Research of Frame and Key Technologies for Intrusion Detection System in IEEE 802.11-based Wireless Mesh Networks", International Conference on Complex, Intelligent and Software Intensive Systems, 2008 (CISIS 2008), Barcelona, 4-7 March 2008, pp. 455 - 460.

[9] Makaroff, D., Smith, P., Race, N.J.P., Hutchison, D., "Intrusion detection systems for community wireless mesh networks", 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2008 (MASS 2008), Atlanta, GA, USA, pp. 610-616.

[10] Wang, X., Wong, J.S. Stanley, F., and Basu, S., "Cross-Layer Based Anomaly Detection in Wireless Mesh Networks", Ninth Annual International Symposium on Applications and the Internet, 2009 (SAINT'09), Bellevue, WA, 20-24 July 2009, pp. 9-15.

[11] Hugelshofer, F., Smith, P., Hutchison, D., Race, N.J.P. "OpenLIDS: A Lightweight Intrusion Detection System for Wireless Mesh Networks", Proceedings of the 15th annual international conference on Mobile computing and networking (MobiCom'09), New York, NY, USA, 2009, DOI: 10.1145/1614320.1614355.

[12] Yang, Y., Zeng, P., Yang, X., and Huang, Y., "Efficient Intrusion Detection System Model in Wireless Mesh Network", 2010 Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC 2010), 24-25 April 2010, pp. 393-396.

[13] Wang, Z., Chen, J., Liu, N., Yi, P., and Zou, Y., "An Intrusion Detection System Approach for Wireless Mesh Networks Based on Finite State Machine", Draft available at: http://www.cs.ucla.edu/~wangzy/inestablishment/resource/IDS_draft.pdf (last accessed March 24, 2012)

[14] Khan, S., Loo, K.-K., and Din, Z.U., "Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks", The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010, pp. 435-330.

[15] Cheikhrouhou, O., Laurent-Maknavicius, M., and Chaouchi, H., “Security Architecture in a Multi-hop Mesh Network”, 5th Conference on Safety and Architectures Networks SAR 2006, Seignosse, Landes, France, June 2006, pp. 1-10.

[16] Shila, D.M. and Anjali, T., “A Game Theoretic Approach to Gray Hole Attacks in Wireless Mesh Networks”, in Proc. IEEE MILCOM, San Diego, CA, Nov. 16-19 2008, pp. 1-7.

[17] Shila, D.M., Cheng, Y. and Anjali, T., “Channel-Aware Detection of Gray Hole Attacks in Wireless Mesh Networks”, The Proceedings of IEEE Globecom 2009, Nov. 30 2009-Dec. 4 2009, Honolulu, HI, USA, 2009, pp. 1-6.

[18] Parno, B., Perrig A., Gligor, V., “Distributed Detection of Node Replication Attacks in Sensor Networks”, Proceedings of the 2005 IEEE Symposium on Security and Privacy (S&P’05), 8-11 May 2005, pp. 49-63.

[19] Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., and Belding-Royer, E.M., “A Secure Routing Protocol for Ad Hoc Networks”, Proceedings of the 10 th IEEE International Conference on Network Protocols (ICNP’02), 12-15 Nov. 2002, pp.78-87.

[20] Salem, N.B. and Hubaux, J.P., “Securing Wireless Mesh Networks”, IEEE Wireless Communication, Volume: 13, Issue: 2, April 2006, pp. 50-55.

[21] Srivastava, V., Neel, J., MacKenzie, A.B., Menon, R., DaSilva, L. A., Hicks, J. E., Reed, J. H., and Gilles, R.P., “Using game theory to analyze wireless ad hoc networks”, IEEE Communications Surveys & Tutorials, Fourth Quarter 2005, Volume 7, No. 4, 2005, pp. 46-56.

[22] Javidi, M.M. and Aliahmadipour, L., “Game theory approaches for improving intrusion detection in MANETs”, Scientific Research and Essays, Vol. 6 (31), 16 December 2011, pp. 6535-6539.

[23] http://www.mathworks.com/products/matlab/

[24] Kindy, D.A. and Pathan, A.-S.K., “A Walk through SQL Injection: Vulnerabilities, Attacks, and Countermeasures in Current and Future Networks”, Building Next-Generation Converged Networks: Theory and Practice, ISBN: 9781466507616, CRC Press, Taylor & Francis Group, USA, 2013. (To Appear)

[25] Khanam, S., Saleem, H.Y., and Pathan, A.-S.K., "An Efficient Detection Model of Selective Forwarding Attacks in Wireless Mesh Networks", Proceedings of the 5th IDCS 2012, 21-23 November 2012, Wu Yi Shan, Fujian, China, Lecture Notes in Computer Science (LNCS), Volume ????, Springer-Verlag 2012, pp. ?–??, 2012. (To Appear)

[26] Mohammed, M. and Pathan, A.-S.K. Automatic Defense against Zero-day Polymorphic Worms in Communication Networks. ISBN 9781466557277, CRC Press, Taylor & Francis Group, USA, 2013. (To Appear)