Arab J Sci Eng (2016) 41:1161–1172
DOI 10.1007/s13369-015-1963-8

RESEARCH ARTICLE - COMPUTER ENGINEERING AND COMPUTER SCIENCE

Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol

K. Geetha[1] · **N. Sreenath**[2]

Received: 28 March 2015 / Accepted: 16 November 2015 / Published online: 17 December 2015

Abstract Mobile ad hoc networks (MANETs) play a vital role in ubiquitous computing. Multimedia communication is the main aspect of MANETs in emergency networks. Security is the major concern in such networks. MANETs are prone to many security problems because of their dynamic changing nature. One of the main attacks that affect any communication in a MANET is the denial-of-service attack. In this paper, such an attack called SYN flooding attack and its detection method are discussed. The presence of the SYN flooding attack in networks may not be identified correctly at an early stage. This leads to the denial of legitimate services at the multimedia server. An algorithm is presented in this paper to detect the presence of the SYN flooding attack at an early stage. The malicious node, instead of launching the SYN flooding attack, may try to delay the communication. This algorithm also finds such malicious nodes which try to affect the multimedia communication in MANETs by introducing unnecessary delays. The solution method involves game theory to form a game between the malicious node and the multimedia server node. The performance of the detection algorithm is verified by analyzing the various quality of service parameters relevant to multimedia communication.

Keywords MANETS · Security · SYN flooding attacks · Game theory · QoS parameters

✉ K. Geetha
kl.geetha@gmail.com

[1] Department of Computer Science, Periyar Government Arts College, Cuddalore, India

[2] Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India

1 Introduction

Mobile ad hoc networks are conveniently used for multimedia communication. In emergency situations like in natural or manmade disasters, in ad hoc services of military, and in educational services, the multimedia communication over MANETs is inevitable. Multimedia communications can be live content transfer or stored information transfer. The data may be transferred through a streaming technique or downloading technique. Streaming technique allows the content play simultaneously with data transfer. But, in the downloading technique, the content can be played only after the entire file is downloaded. The multimedia content can be distributed by a client–server model or by a peer-to-peer technique. In client–server model, a single node transfers data to all. In peer-to-peer technique, one node communicates with another node. Some multimedia transmissions may not need the user participation. In some other communications, the user needs to participate in the communication. In all the cases, the successful communication of the multimedia data depends on the satisfaction of the receiver user. Since the user satisfaction is a non-measurable quality, certain QoS parameters can be analyzed which reveals the effective transfer of data to the user

Generally, the multimedia communication is delay sensitive. Once the communication of multimedia data started from the source, the receiver wishes to receive the data continuously without any delay in between the adjacent frames. In order to provide good multimedia communication, the source should ensure a speedy and safety multimedia transfer to the receiver user. The malicious user may launch several attacks to affect the quality of transfer. The well-known MANET attacks and their effect on multimedia communication are listed in Table 1.

The very common and most dangerous attack is one of the denial-of-service (Dos) attack called SYN flooding attack.

Table 1 MANET attacks

Slno	Attack	Description	Effect on multimedia communication
1	Jellyfish attacks [1]	Jellyfish attackers intrude the network first and then delay the packets before forwarding them	Delay and jitter increases
2	Flooding attack [1]	A lot of RREQ s to a node which does not exist in the network. The request will be flooded wasting others battery power and the bandwidth	Denial of service and decreased throughput
3.	Black hole attack [2]	Malicious node is sending fake information that it is having an optimum route to destination. All nodes send information through the malicious node, which discards the messages along with control packets	Increases packet loss and decreased packet delivery ratio
4	Gray hole attack [2]	Malicious nodes selectively forward packets	Increased packet loss, decreased throughput, and increased delay
5	Link spoofing attack [3]	A malicious node advertises wrong routing information with the neighbor. In particular in OLSR protocol, wrong MPRs were chosen for relay. This leads to dropping or modifying of routing traffic	Decreased throughput and packet delivery ratio
6	Worm hole Attack [4]	Two misbehaving nodes cooperate by using private high-speed network. Try to transfer data with high speed. The other nodes use this path after words. The data are then misused	Decreased throughput
7	SYN flooding attack [29]	Malicious nodes send a lot of SYNs and do not send the final acknowledgment to the ACK sent by the genuine node	Denial of service. Increased delay and jitter, and decreased throughput

This attack affects the entire data transfer by denying the legitimate services of the source node.

Our aim is to provide a safety and speedy multimedia communication from the source node to destination using the AODV protocol; we would like to propose solution for the detection of SYN flooding attacks. This proposed mechanism not only detects the attack but also detects the source of the attack and the delay introducers.

The paper is organized as follows. In Sect. 2, the SYN flooding attacks are discussed. Section 3 describes the existing methods to find out the SYN flooding attacks. Section 4 gives an introduction to game theory and the environment of the multimedia transfer. Section 5 discusses the game theoretical algorithm and the proposed method for the detection of SYN flooding attacks. In Sect. 6, the simulation is explained; the various QOS parameters are analyzed to check the efficiency of the detection method, and the conclusion is presented in Sect. 7.

2 SYN Flooding Attacks

In normal mode of operation, the node which acts as multimedia server (MS) listens for the SYN from the connection initiator. The connection initiating node sends a SYN to MS node first. The MS node acknowledges with a SYN–ACK. This state is a half-open state. The half-open connection information is maintained by the MS node in a backlog queue. Later, the connection initiator acknowledges the SYN–ACK sent by the MS node with a final ACK. This is how the Transmission Control Protocol initiating a transfer with three way handshake as shown in the Fig. 1.

In an attack mode, the connection initiator sends multiple SYNs to MS node. MS node responds to all SYNs by SYN acknowledgment. The connection initiator may not respond with final acknowledgment. Instead a lot of SYNs are repeatedly sent from the connection initiating node. The backlog queue will be filled with many half-open connections. This makes the MS node to deny further legitimate connections as shown in the Fig. 2.

3 Existing Methods

Many of the existing methods use some common techniques like SYN cache method, probing scheme method, change point detection, bloom filters and list-associated methods, mathematical methods, statistical methods, and intentional dropping methods to detect the SYN flooding attacks. Method using SYN cache [5] allocate minimum resources for the half-open connections. The complete allocation of resources takes place after the connection is established.

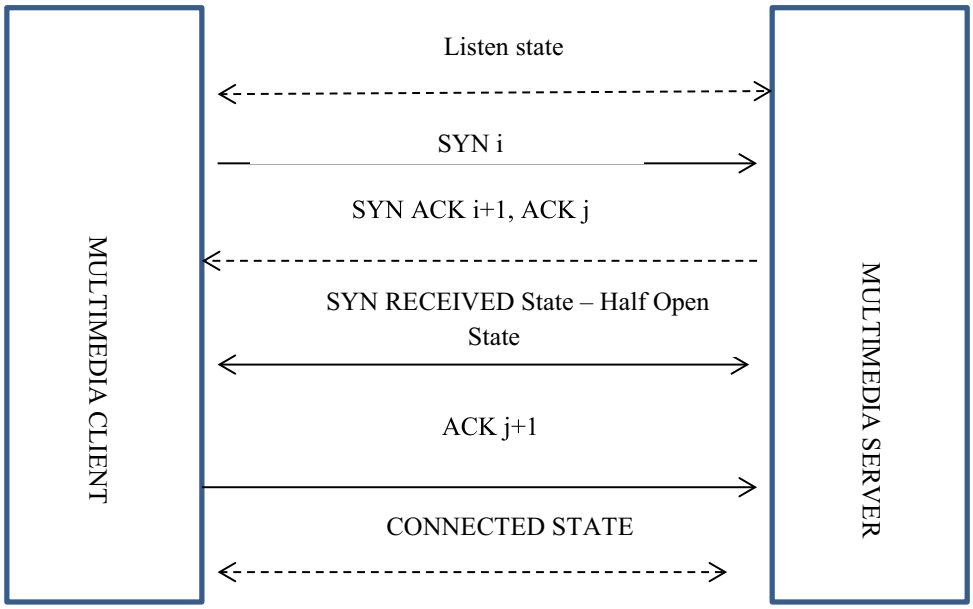

Fig. 1 TCP-three way handshake

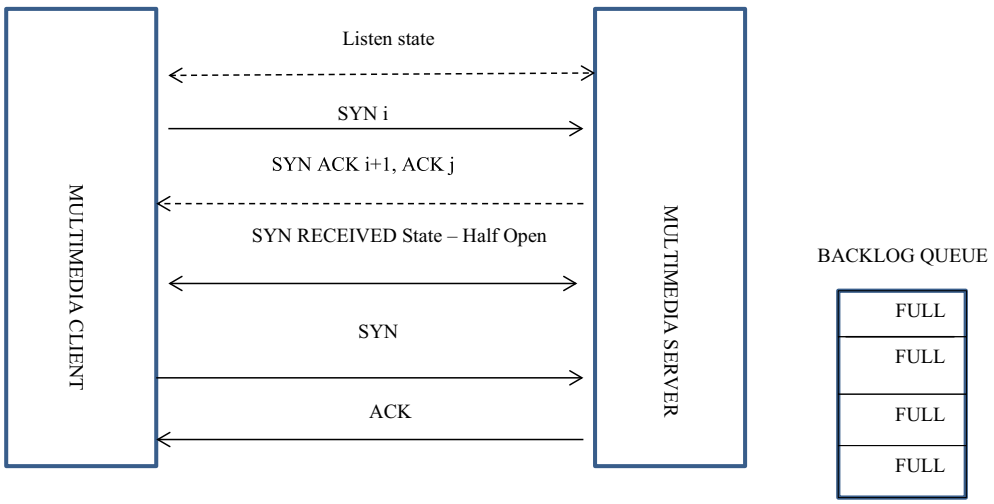

Fig. 2 SYN flooding attack

Methods using probing scheme: Xia et al. [6], proposed method based on probing scheme that ensures the efficient early detection. The method used half-open connections to identify the attack. Yang et al. [7] considered the network traffic delay as additional parameter to identify the attack.

Methods using change point detection: Siris et al. [8], Wang et al. [9], Harris et al. [10], Osman et al. [11] detected the anomaly in the network traffic with their change point detection algorithm along with CUSUM algorithm. Alexander et al. [12] also used the change point detection method in the random observations of network traffic.

Bloom filters and list-associated methods: Changua et al. [13], Chen, Wei et al. [14]. Hu et al. [15]. They used the SYN and ACK pair and the difference between them as important parameter for detection. Ling et al. [16] maintained a list along with mapping table and hash functions, whereas a white list was used by Kim et al. [17] for storing the legitimate addresses to detect the attack, with threshold checking technique.

Mathematical and statistical methods: Divakaran et al. [18], Janowski et al. [19], Ranjan et al. [20], Ohsita et al. [21],Wang et al. [22], Bellaiche et al. [23] used mathematical or statistical techniques to detect the attack.

Intentional dropping methods: Jindou et al. [24], Basheer et al. [25] intentionally dropped the first SYN packet of each connection request.

Jelena et al. [26] presented D-WARD (DOS network Attack Recognition and Defense), a source defends against DoS attacks. Garg et al. [27] used a rate controller for resource usage Haggerty et al. [28] detected the SYN flood-

ing attack using a pre-filter node (PF). Schuba et al, [29] analyzed completely the SYN flooding attacks.

These traditional methods of SYN flooding attack detection do not provide a quantitative decision making. This proposed method considers the cost as important factor in multimedia data transfer for which game theory is used for the detection. The cost or benefit of the network and the attacker is analyzed by finding at the most benefit status called NASH equilibrium which is a state or optimum solution for the players. The connection initiator and the attacker are viewed as two competing players of a game. Different strategies like, to-attack, to-defend, to-be-idle, and to-delay are considered which requires a game theoretical approach to the problem. The early detection of the attack is possible by checking the destination node at the time of sending acknowledgment. If it is malicious, the connection is closed. The intermediate nodes are verified later. The method not only detects the SYN flooding attack, but the source of the attack is identified as malicious node. Besides the identification of the SYN flooding attacks, our method also detects nodes which send delayed ACKs continuously. This helps in facilitating a speed and safe multimedia communication.

The main parameter for any multimedia message transfer is user satisfaction which can be analyzed by analyzing the quality of service parameters (QoS) with our detection algorithm. The user satisfaction in multimedia communication is mainly dependent on the jitter which is the delay between adjacent packets received. The proposed method gives special focus to the delay and jitter as special parameters.

4 Game Theory and Security

Game theory [30,31] is the branch of mathematics concerned with the analysis of strategies for dealing with competitive situations. Game theory has been applied to contexts in war, business, Biology and also in Economics, Political Science, and other related fields.

Many methods apply game theory to the security of networks. Agah et al. [32,33] present an intrusion detection system (IDS) using game theory. Emmanouil Panaousis et al. [34] suggested an intrusion detection system with game theory. The same authors suggested a game theoretic approach called [35] AODV-GT (AODV-Game Theoretic) to provide defense against black hole attacks.

Let G be a game with $G = (\mathrm{St}, \mathrm{Ut})$

where St is the set of strategy profiles and Ut is the set of payoff profiles

Each player i in $\{1, 2, \ldots, n\}$ has the strategy s_i and produces the strategy profile

$\{s_1, s_2, \ldots..s_n\}$.

The player gains the utility $U_i(S)$ by choosing a strategy s_i.

$$s_i \in \arg\max_{s_i \in S_i} U_i\,(s_i, s_{i'}) \;\; \forall i \in \{1, 2, \ldots n\} \tag{1}$$

$s_{i'}$ be the strategy of the player except i

A strategy profile $s^* \in S^*$ is a NE if,

$$\forall i, u_i\left(s_i^*, s_{i'}^*\right) \geq u_i(s_i, s_{i'}^*) \tag{2}$$

A two-player non-cooperative nonzero sum game is defined here between the MS node and the malicious node. The game is non-cooperative because the players take their decisions on their own independently. The game is also a nonzero sum game which means the gain or loss of one player does not affect the other player's gain or loss. The nodes in the network are defending even if the malicious node is not attacking.

In order to find the NASH equilibrium (NE) in a nonzero sum game, we have to consider the dominant strategy. A strategy is called dominant when it is better than any other strategy. In mathematics, for any player i, a strategy $S^* \in S_i$ dominates another strategy $s' \in$ Si if $\forall s_{i'} \in S_i$

$$u_i\left(s^*, s_{i'}\right) \geq u_i\left(s', s_{i'}\right) \tag{3}$$

5 Environment of the Proposed Method—GT-IDS-DJ Method

The proposed method is implemented as an intrusion detection system (IDS). There are two types of IDS [36] as (i) Network IDS—This works on the information obtained from the network traffic (ii) Host IDS—This works on the information from the host. As any node in MANET can act as multimedia server, this IDS is a host-based IDS which runs on every node.

The SYNs, ACKs, half-open connections, and neighbor nodes information are monitored by a monitor segment. The detection algorithm can be executed either at the time of sending ACKs or at the time of half-open connections exceeding the threshold value. In order to avoid the connection establishment delay, we execute the algorithm when the half-open connections exceed the threshold value T which can be calculated by adaptive threshold [8] method at nth interval as $T_n = (\alpha+1)m$, where $\alpha > 0$ is a value that indicates the percentage of half-open connections above the mean half-open connections that we consider as the attack behavior and m is the mean value of previous half-open connection values.

The half-open connections can be computed as,

$$\mu = \mathrm{NS_{syn}}/\mathrm{NR_{Ack}}$$

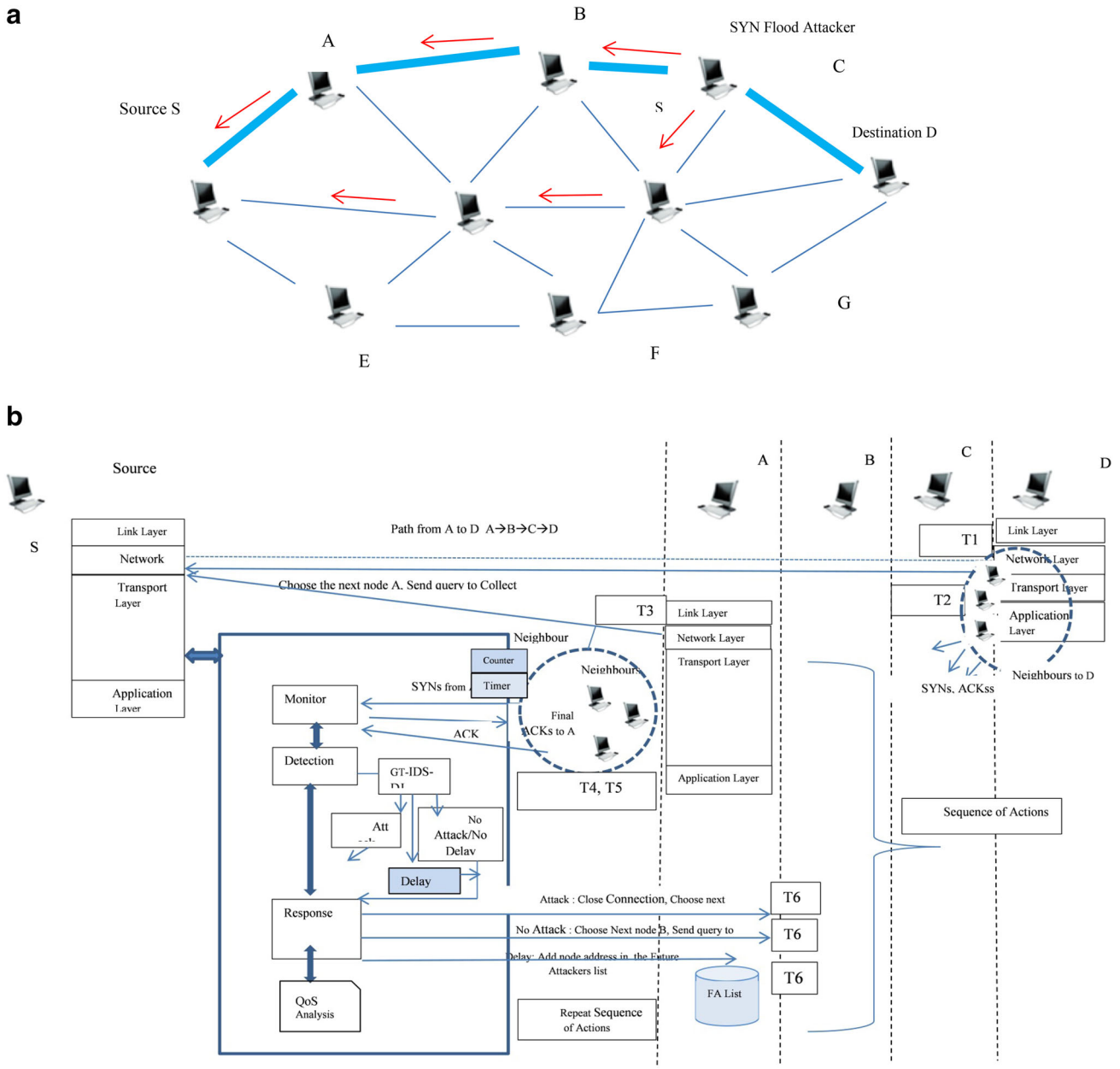

Fig. 3 **a** MANET with source, destination and attacker. **b** Sequence diagram with GT-IDS-DJ

where NS_{syn} = number of SYN acknowledgements sent, NR_{Ack} = number of final acknowledgements received.

The "μ" is verified for every time interval "t." If all the final acknowledgments are received by a source, μ will be 1. If the final acknowledgements are not received properly, half-open connections will increase in number, and the μ value will be greater than one.

Every node is assumed to maintain a list of one-hop neighbor nodes. This should be updated periodically. First, the source node obtains the neighbor nodes of the destination with a query. Then, it computes the SYNs and ACKs which are sent from the destination node through the neighbors. The source "S" forms a non-cooperative game between itself and the destination node. If the destination is not an attacker, the source node starts verifying the intermediate nodes starting from the first available intermediate node in its path.

In the Fig. 3a, it is assumed that C is a malicious node sending many SYN packets to S. D is the connection initiator. The IP address of the connection initiator which is sending the SYN is verified by the source before sending acknowledgment. If the IP address is reachable, then the ACK will be sent to the node. Otherwise, the SYNs will not be acknowledged by the source. Starting from the node S the control

packets will be transmitted by choosing the next node and after checking whether the node is malicious. This is performed by obtaining the neighbor nodes of the intermediate nodes and computing the numbers of SYNs sent through the neighbor node from the intermediate node. A game is formed between MS node and the intermediate node. The IDS can check for the attack with following motives.

1. To ensure safety of the source. (Verifying the source whether it is being affected)
2. To provide a safe route to the destination. (Verifying the intermediate nodes whether they are attackers)
3. To ensure the validity of the destination. (Verifying whether the message is communicated to a genuine node)

It is clear from the sequence diagram given in the Fig. 3b, that, at time T_1, the next node is given by the routing protocol in between the source "S" and destination "D." The source node "S" sends a query to "D" and obtains the neighbor node addresses. At time T_2, the SYNs, ACKs, sent through neighbor nodes to "S" is computed. A game is formed to check whether "D" is an attacker or a delay introducer. If the destination is not an attacker or delay introducer, at time T_3, query is sent to the first intermediate node "A" in the path in order to get the neighbors of "A." "A" sends the neighbor nodes list at time T_4. At time T_5, the information regarding the number of SYNs sent from "A" to "S," the number of final ACKs sent from "A" to "S" is obtained. With this information, a game is formed by the source "S," between itself and "A" by the detection module. The response module decides the type of response such as to close the connection or to continue with the sequence of actions

The sequence of checking are carried out as follows.

- First the address of the destination node is verified whether it is existing
- If it exists, the destination node is verified for SYN flood attacker or delay introducer. The intermediate nodes are verified for the presence of attackers or delay introducers.
- If destination does not exist, the destination address is assumed to be spoofed and the malicious node which spoofed the address is located as SYN flood attack generator. This is necessary in case if the IDS is called with half-open connections exceeding threshold value.

As a special case, monitor segment also keeps a list of ACKs along with the time it is received. If the final ACK for a particular node is received continuously with delay, these nodes are added into the future attackers list (FA list) as delay introducers and connections are closed with them. This is considered in order to reduce the delay and jitter in the multimedia communication.

Generally, the TCP SYN flood attacks are generated by spoofing the address. The attackers choose the address such that the spoofed address will be a non-reachable address. Sometimes, genuine IP address may also be spoofed. In both the cases, any node has to send the SYNs only through the neighbor nodes. The neighbor nodes will help to detect the actual attacker which sends a lot of SYNs through them. Since the detection here is performed by analyzing the traffic near the source of the attack, the attacker cannot be escaped.

5.1 The Attack Detection

The method is game theory-based intrusion detection with minimum delay and jitter (GT-IDS-DJ). The monitor collects the data of the network and check for malicious activities. A security game is formed as G_s.

Step 1: Forming the game between attacker and multimedia server

Goal of the attackers is to attack the multimedia server, and goal of the multimedia server is to transfer the multimedia data with security to the receiver. If there is attack, the multimedia server is the looser wasting its time, energy, and resources.

The strategies are defined as

(D, A), $(D$, Na_Dl$)$, $(D$, Na_Ndl$)$, (Nd, A), (Nd, Na_Dl), (Nd, Na_Ndl)

where D = Defending, A = Attacking, Nd = Non-defending, Na-Dl = No Attack but Delay, Na-Ndl = No Attack No delay.

The utility of the defending and attacking nodes are calculated by forming the payoff matrix as Table 2 [34]. We define $P_d = (p_{d1}, p_{d2}, p_{d3}, \ldots, p_{dn})$ as the probability distribution for defend case over N and

$P_a = (p_{a1}, p_{a2}, p_{a3}, \ldots, p_{an})$ as the probability distribution for attack case over N. We compute the utilities of a particular node n_i with the following metrics $P_w = (p_{w1}, p_{w2}, p_{w3}, \ldots, p_{wn})$ as the probability distribution for delay introduced case over N.

The following assumptions are made.

$$\sum_{n\in N} p_{dn} \le P_d \quad \sum_{n\in N} p_{wn} \le P_w \quad \text{and} \quad \sum_{n\in N} p_a n \le P_a$$

r_{da} is the rate of detection of the attack, r_f is the false alarm rate, r_{dw} is the rate of detection of the intentional delay introduced by the attacker node, cost $_w$ is the cost of introducing delay, cost d_w is the cost involved for handling the delay, cost $_f$ is the false alarm handling cost, cost $_a$ is the cost of producing attack, cost $_{da}$ is the cost of defending the attack.

Total security loss due to attack is S

$$0 \leq r_{\text{da}}, r_f, r_{\text{dw}}, \text{cost}_{\text{dw}}, \text{cost}_a, \text{cost}_{\text{da}}, \text{cost}_f, \text{cost}_w \leq 1$$

[Hint: In the payoff matrix (PM), for every defending category, the rate of detection of the attack and the rate of detection of the delay are subtracted from the total probability 1, and this is multiplied with the total security S. It is true for all the defending cases.]

Step 2: Finding the utility of an attacker and the defender
The utility functions for MANET $\text{Ut}_{\text{MANETt}}$, and attacker Ut_{ATT} are calculated for a node n_i from the given Table 2 as,

$$\begin{aligned}&\text{Ut}_{\text{MANET}}(p_d, p_a, p_w)\\&= \sum_{\text{ni}\in N}[(D, A)_{\text{Def}} + (D, \text{Na\_Dl})_{\text{Def}}\\&\quad + (D, \text{Na\_Ndl})_{\text{Def}} + (\text{Nd}, A)_{\text{Def}}]\end{aligned}$$

where
Def is the defending strategy

$$\begin{aligned}&(D, A)_{\text{Def}} = p_{d,\text{ni}}\, p_{a,\text{ni}}\, (-(1 - r_{\text{da}} - r_{\text{dw}})\, S_{\text{ni}}\\&\quad - r_{\text{f}}\text{cost}_{\text{f}}\, S_{\text{ni}} - \text{cost}_{\text{da}} S_{\text{ni}} - \text{cost}_{\text{dw}} S_{\text{ni}})\\&(D, \text{Na\_Dl})_{\text{Def}} = p_{d,\text{ni}}\, p_{w,\text{ni}}\, (-(1 - r_{\text{da}} - r_{\text{dw}})\, S_{\text{ni}}\\&\quad - (\text{cost}_{\text{da}} + \text{cost}_{\text{dw}}) S_{\text{ni}})\\&(D, \text{Na\_Ndl})_{\text{Def}} = p_{d,\text{ni}}\, \left(1 - \left(p_{a,\text{ni}+} p_{w,\text{ni}}\right)\right.\\&\quad \left.(r_f \text{cost}_f\, S_{\text{ni}} - \text{cost}_{\text{da}} S_{\text{ni}} - \text{cost}_{\text{dw}} S_{\text{ni}})\right)\\&(\text{Nd}, \text{A})_{\text{Def}} = \left(1 - p_{d,\text{ni}}\right)\, p_{a,\text{ni}}\, (-S_{\text{ni}})\end{aligned}$$

The Ut_{MANET} equation is given by,

$$\begin{aligned}\sum_{\text{ni}\in N} S_{ni}\, &\left[p_{d,ni}\, p_{a,ni}\, \left(-(1 - r_{\text{da}} - r_{\text{dw}}) - r_f cost_f - cost_{\text{da}} - cost_{\text{dw}}\right)\right.\\&+ p_{d,ni}\, p_{w,ni}\, (-(1 - r_{\text{da}} - r_{\text{dw}} - cost_{\text{dw}} - cost_{\text{da}}))\\&\left.+ p_{d,ni}\, \left(1 - p_{a,ni} - p_{w,ni}\right)\, \left(-r_f cost_f - cost_{\text{da}} - cost_{\text{dw}}\right) + p_{a,ni}\, \left(-1 + p_{d,ni}\right)\right] \quad (4)\end{aligned}$$

$$\begin{aligned}\text{Ut}_{\text{ATT}}(p_{\text{d}}, p_{\text{a}}, p_{\text{w}}) = \sum_{\text{ni}\in N} &\left[(D, A)_{\text{Att}} + (D, \text{Na\_Dl})_{\text{Att}}\right.\\&\left.+(\text{Nd}, A)_{\text{Att}} + (\text{Nd}, \text{Na\_Dl})_{\text{Att}}\right]\end{aligned}$$

where Att is the attacking strategy

$$\begin{aligned}&(D, A)_{\text{Att}} = p_{d,\text{ni}}\, p_{a,\text{ni}}\, (1 - r_{\text{da}} - r_{\text{dw}} - \text{cost}_a)\, S_{\text{ni}}\\&(D, \text{Na-Dl})_{\text{Att}} = p_{d,\text{ni}}\, p_{w,\text{ni}}\, (1 - r_{\text{da}} - r_{\text{dw}} - \text{cost}_w)\, S_{\text{ni}}\\&(\text{Nd}, A)_{\text{Att}} = \left(1 - p_{d,\text{ni}}\right)\, \left(p_{a,\text{ni}}\right)\, (1 - \text{cost}_a)\, S_{\text{ni}}\\&(\text{Nd}, \text{Na-Dl})_{\text{Att}} = \left(1 - p_{d,\text{ni}}\right)\, p_{w,\text{ni}}\, (1 - \text{cost}_w)\, S_{\text{ni}}\end{aligned}$$

The Ut_{Att} equation is given by,

$$\begin{aligned}\sum_{\text{ni}\in N} S_{\text{ni}}\, &\left[p_{d,\text{ni}}\, \left(p_{a,\text{ni}}(1 - r_{\text{da}} - r_{\text{dw}} - \cos t_a)\right.\right.\\&+ \left.p_{w,\text{ni}}(1 - r_{\text{da}} - r_{\text{dw}} - \cos t_w)\right)\\&+ (1 - p_{d,\text{ni}})(p_{a,\text{ni}}(1 - \cos t_a) + p_{w,\text{ni}}(1 - \cos t_w))\left.\right] \quad (5)\end{aligned}$$

Step 3: Defining the possible strategy space of an attacker and defender
We define the strategy space for forming our game between the server and the malicious node and find the NASH equilibrium by forming the bi matrices [35] for the attacker and defender.

Strategy space of the MANET:

D_i: the MANET defends this node i
$D_{i'}$ the MANET defends any other node i'

Strategy space of a SYN flood attack node:

A_i: the SYN flood attack node attacks this node i
Na-Dl_i: the SYN flood attack node pretends an attack which increases the delay.
Na-Ndl_0: the SYN flood attack node does not attack
A_h: the SYN flood attack node attacks any other node h.
Na-Dl_h: SYN flood attack nodes pretends an attack to any other node and increases the delay

The MANET has the potential to play with,

$$D = \left(D_i, D_i D_i, D_{i'}, D_{i'}\right)$$

The node has potential to attack with

$$A = \begin{bmatrix}\text{Ai}\\ \text{Na-Dli}\\ \text{Na-Ndl0}\\ A_h\\ \text{Na-Dl}_h\end{bmatrix}$$

Table 2 Payoff matrix

Strategy	Attacking	Introducing intentional delay	Non-attacking non-delaying
Defend	$(D, A) = (-(1 - r_{da} - r_{dw})\text{Sn}_i - r_f \text{cost}_f \text{Sn}_i - \text{cost}_{da}\text{Sn}_i - \text{cost}_{dw}\text{Sni}, (1 - r_{da} - r_{dw})\text{Sn}_i - \text{cost}_a\text{Sn}_i)$	$(D, \text{Na\_Dl}) = (-(1 - r_{da} - r_{dw})\text{Sn}_i - \text{cost}_{da}\text{Sn}_i - \text{cost}_{dw}\text{Sni}, (1 - r_{da} - r_{dw})\text{Sn}_i - \text{cost}_w\text{Sn}_i)$	$(D, \text{Na\_Ndl}) = (-r_f \text{cost}_f \text{Sn}_i - \text{cost}_{da}\text{Sn}_i - \text{costd}_w\text{Sni}, 0)$
Non defend	(Nd, A) = $(-\text{Sn}_i, \text{Sn}_i - \text{cost}_a\text{Sn}_i)$	(Nd, Na_Dl) = $(0, \text{Sni} - \text{cost}_w\text{Sn}_i)$	Nd,Na_Ndl) = (0, 0)

Table 3 Payoff matrix for defend case—multimedia server

Strategy tuple	A_i	Na-Dl_i	Na-Ndl_0	A_h	Na-Dl_h
Di	$\text{Ut}(t) - \text{Dc}_i$	$\text{Ut}(t) - \text{Dc}_i - \text{Dw}_i$	$\text{Ut}(t) - \text{Dc}_i$	$\text{Ut}(t) - \text{Dc}_i - \text{Fc}_h$ for $h \neq i$	$\text{Ut}(t) - \text{Dc}_i - \text{Dw}_h - \text{Fw}_h$ for $h \neq i$
Di′	$\text{Ut}(t) - \text{Dc}_{i'} - \text{Fc}_i$	$\text{Ut}(t) - \text{Dc}_i - \text{Dw}_{i'} - \text{Fwi}$	$\text{Ut}(t) - \text{Dc}_{i'}$	$\text{Ut}(t) - \text{Dc}_{i'} - \text{Fc}_h$ for $h \neq i, i'$	$\text{Ut}(t) - \text{Dc}_{i'} - \text{Dw}_{i'} - F_{\text{Wh}}$ for $h \neq i, i'$

Table 4 Payoff matrix for attack case—attacker

Strategy tuple	A_i	Na-Dl_i	A_0	A_h	Na-Dl_h
Di	$B_{\text{Att}}(t) - \text{CA}_i$	$B_{\text{Att}}(t) - \text{CA}_i$	0	$B_{\text{Att}}(t) - \text{CA}_h$ for $h \neq i$	$B_{\text{Att}}(t) - \text{CA}_h$ for $h \neq i$
$D_{i'}$	$B_{\text{Att}}(t) - \text{CA}_i$	$B_{\text{Att}}(t) - \text{CA}_i$	0	$B_{\text{Att}}(t) - \text{CA}_h$ for $h \neq i$	$B_{\text{Att}}(t) - \text{CA}_h$ for $h \neq i$

$A_0 = \text{Na-Ndl}_0$

The benefit of the attacker (B_{Att}), the utility value of the MANET PD, is calculated from the total SYN packets received by MS and sent by client. Attack cost (CA) is estimated from the SYNs sent by the client additionally, and defend cost is estimated from the intrusion detection system (IDS).

We form the payoff matrix for defending case as given in Table 3

The $\text{Ut}(t)$ can be calculated from Ut_{MANET} from (4), where the defending cost Dc_i is the cost of establishing and running IDS for the network. The Fc_i the false alarm handling cost, while Fw_i is the cost of handling the false alarm produced for the delay made by the attacker node.

The defending cost is calculated from the intrusion detection system. It depends on the number of neighbor nodes.

The attacker has five strategies and the payoff matrix for the attack case is given by the Table 4.

The difference between the cost spent for introducing delay and the cost spent for an attack is negligible and treated the same. But the benefit earned by the attacker with a launch of attack is the entire security loss, and it is NULL in the case with a delay introduction. The delay introduction affects only the user satisfaction and not the security.

Step 4: Finding NASH equilibrium

The utility of the MANET (Ut_{MANET}) is computed from (4). The benefit of the attacker is the loss of security (S) to MANET due to a successful attack which is Ut_{Att} from (5).

It is assumed that the cost of generating the attack $< S$. Otherwise the attacker will not attack. The benefit of the attack is a combination of the delay introduced γ due to the attack together with the loss of security S which can be represented as a linear equation as

$$\text{B}_{\text{Att}} = \gamma + \text{S} \tag{6}$$

We find the Nash equilibrium (NE) of the game by finding the dominant strategy by setting the values from (3), the row i is dominating j if a $(i, j) \geq a(j, k)$ for $j = 1, 2, 3 \ldots n$.

In Table 3, d_1 is obviously dominating d_2, d_5 and hence d_2, d_5 can be eliminated. $d_{11} = d_{13} >= d_{14}$.

If Defending Cost(i) > Defending Cost(i')$_\prime$ then $d_{13} > d_{11}$

If Defending Cost(i')$_\prime$ >Defending Cost(i) then $d_{11} > d_{13}$

In Table 4, $a_1 = a_2, a_4, a_5$. But, the benefit for the attacker due to increasing the waiting time in a node is lesser than the benefit obtained for the attacker due to an attack. From (6), the benefit of the attacker after increasing the delay is $B_{\text{Att}} = \gamma + 0$ (since there is no security loss).

In an attack case, the delay is added with loss of security

So, at any time

$$a_1 > a_2, a_4, a_5$$

So, (d_1, a_1) is the NASH equilibrium.

At NE, the attack potential and defend potential reaches maximum above which a node cannot change the values for getting maximum utility.

Step 5: Finding the potential of a node
The potentials of malicious nodes to attack the server, keeping NE as a standard, are calculated. If this is high, we assume the node is a malicious node, and we will close the connection with the malicious node and choose the next available node from the next available route.

The expected potential of the defend case, attack case, and intentional delay are calculated.

Potential of defend case (this node)DF_i

$$= D_i \left(\sum_x A_x + \sum_y \mathrm{Na\_Dl}_y \right) \tag{7}$$

Potential of defend case (any other node) $\mathrm{DF}_{i'}$

$$= D_{i'} \left(\sum_x A_x + \sum_y \mathrm{Na\_Dl}_y \right)$$

$$\forall x = i, 0, h \text{ and } y = i, h \tag{8}$$

Potential of attack case (this node) $A_i = A_i \sum_z D_z$ (9)

Potential of attack case (no attack) $A_0 = A0 \sum_z D_z$ (10)

Potential of attack case (any other node) $A_{h=}\mathrm{A_h} \sum_z D_z$ (11)

Potential to increase delay-this node = $\mathrm{Na\_Dl}_i \sum_z D_z$ (12)

Potential to increase delay-any other node_$\mathrm{Na_Dl}_h \sum_z D_z$ (13)

$\forall z = i, i'$

If the potential of the node to attack is higher than defending potential of the node, then that node is identified as misbehaving node. The nodes which increase the delay are calculated by checking the potential to delay. If the potential to delay is beyond a threshold value these nodes are identified as nodes which increase delay. These nodes are added to the block list maintained by the monitor segment. The algorithm is given below

5.2 Algorithm

The algorithm works in three phases in the MS node. 1. Monitoring the network 2. Detection of the attack and Maintenance of the future attack list 3. Response Segment.

5.2.1 Monitoring the Network

The monitor segment of the MS node obtains the information regarding the number of SYN packets sent through the neighbor node, number of acknowledgements received and connection established information, number of half-open connections existing, number of acknowledgements sent from the multimedia server to the node, and the number of final acknowledgments sent to the server. Once the information is given to the monitor, the neighbor nodes can refresh the information available with them. If the half-open connections are more the detection algorithm is called for verifying the nodes.

5.2.2 Detection of the Attack, Attacker, and Delay Introducer

The detection segment of the multimedia server after obtaining the increased half-open connections alarm verifies the intermediate nodes toward client whether these nodes are malicious, by calculating the number of SYN packets received, ACKs sent, and final ACKs received. The five steps of the game theoretical detection are carried out.

The monitor updates the information about an intermediate node by obtaining information from its neighboring nodes. Some attackers may not attack but delay the communication. The delayed transfer affects the jitter, and the effect is equivalent to a null transfer in the case of multimedia communication. These two parameters affect the satisfaction of the client very much. If the potential of the attacker is more in introducing the intentional delay, the monitor adds the nodes to a block list and check for future attack from these nodes.

5.2.3 Response Segment

The response segment verifies the result of the detection of the attack. If attack or delay is present, the connection with the malicious node is closed and an alternate node is chosen to form the path. The performance of the network depends on the alternate route chosen for transfer.

6 Criteria for Analyzing the Performance of the Algorithm

Different applications have different quality of service (QOS) parameters. For multimedia communications, delay and jitter are the main parameters [37]. The detection scheme behaves well with these parameters. A simulation is carried out in NS2 with AODV protocol. The simulation parameters are given in Table 5. Since our aim is to test the mechanism with any basic protocol, we have chosen the AODV as the routing protocol.

Table 5 Simulation parameters

Number of nodes	100
Simulation area	1000 m × 1000 m
Buffer size (queue length)	50 Pkts
Packet size	1024 bytes
Application traffic	Video traffic
Simulation time	200 s
Number of connections	50
Connection duration (secs)	20
Data intervel	0.01,0.02,0.03,0.04,0.05,0.06, 0.07,0.08,0.09.1.00
Connection	10,20,30,40,50,60,80,100,120, 140,150
Protocol used	AODV

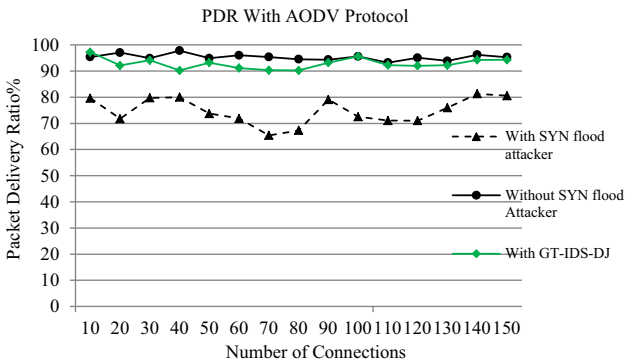

Fig. 4 PDR with AODV protocol

We assume a multimedia data transfer. So, the parameters which are considered important for the multimedia data transfer like packet delivery ratio, control overhead, delay, throughput, and jitter are considered for analysis.

6.1 Packet Delivery Ratio

The packet delivery ratio (PDR) is the ratio of the packets received by the destination to the number of packets sent from the source. Without SYN flood attack, the packet delivery ratio is maximum and even 100 % of data are successfully delivered as shown in Fig. 4. With attacks, the packet delivery ratio is minimum and even below 64 % and when the detection mechanism is implemented the PDR is stable which lies between 90 and 100 % as in Fig. 4.

6.2 Control Overhead

Control overhead is the number of control packets used for sending the messages transmitted over the network. It is expressed in bits per second or packets per second as shown in Fig. 5. This includes requests, replies, and error messages. It measures the scalability of the protocol, and the

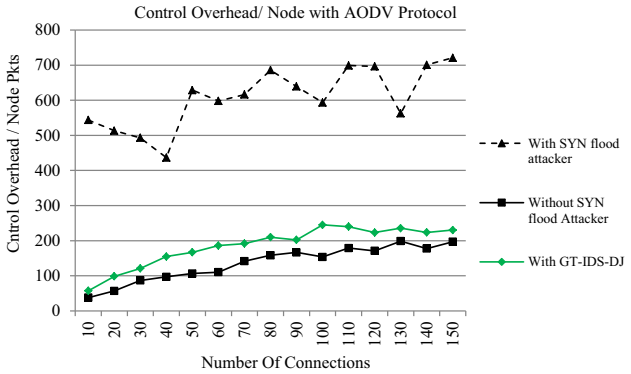

Fig. 5 Control overhead/node with AODV protocol

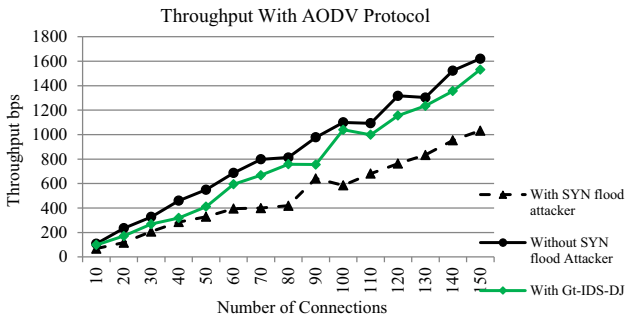

Fig. 6 Throughput with AODV protocol

network. The control overhead is less without attacker. When the SYN flooding attack happens, it reaches maximum. With our detection mechanism, it is very less and even reaches the overhead status without attacker.

6.3 Throughput

It is the number of bits received per second by the destination—the amount of data successfully transferred from source node to destination node. This is explained in Fig. 6. Throughput is maximum and steady in the case if SYN flood attack is not affecting the nodes. After that with detection of the attack by the game theory method though the throughput is not reaching the maximum, it is steady and not decreasing very much as in the case of with attacks. A maximum of 1500 bits per second is produced which is an improvement over the 1000 bps in an attacked situation.

6.4 End-to-End Delay

The time taken by a data packet to reach from source node to destination node is called delay. The end-to-end delay is shown in Fig. 7. It is the ratio of total delay to the number of packets received. With no attacks, the delay is less. It even reaches zero delay. But, with attacks the delay reaches maximum even 90 % and with our game theory detection

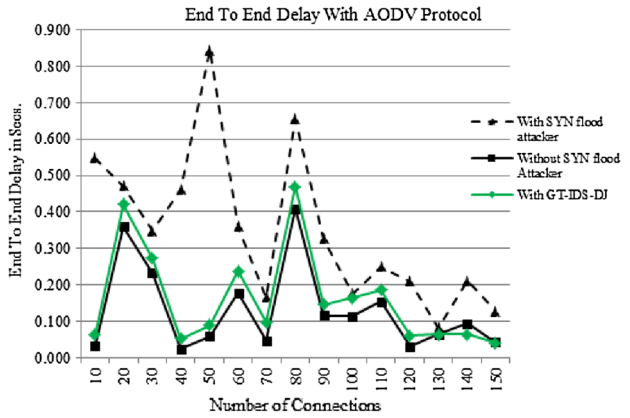

Fig. 7 End-to-end delay with AODV protocol

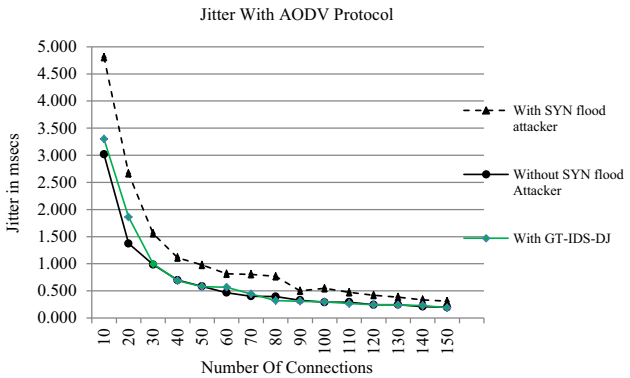

Fig. 8 Jitter with AODV protocol

technique the delay is minimum. This is because of the avoidance of delay introducing nodes.

6.5 Jitter

Jitter is the delay between adjacent packets. The jitter is given in Fig. 8. For multimedia message transfer, this is the main parameter taken into consideration for analysis. If jitter is increased, the quantity of the multimedia transfer is very low. Minimum jitter provides a very good multimedia transfer. In the attack-free scenario, the jitter is very low, but the presence of SYN flood attack increases the jitter. Our game theory detection technique detects the SYN flood attack and eliminates the malicious nodes by which the jitter is also decreased.

7 Conclusion

The intrusion detection system that is available in multimedia server node identifies the attack. The utility considers all the possibilities like detection rate, false alarm, cost of detection, cost of false alarm, defending cost, and attacking cost. The NASH equilibrium is calculated, and the potentials of the attacker to attack and the defender to defend are also calculated. The cost spent toward the protection for a defender and the cost spent toward the attack generation by an attacker can be calculated. From this method, not only the SYN flooding attackers and SYN flooding attacks are identified but also the nodes that intentionally introduce delay to affect the multimedia communication are also detected. They are maintained in a block list for future consideration. The connections with the attackers are closed. This gives full assurance that the node selected for the transfer of data is not malicious and also this node can provide transfer with minimum delay and jitter.

References

1. Nguyen, H.L.; Nguyen, U.T.: A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Netw. **6**1,32–46 (2008)
2. Panaousis, E.A.; Politis, C.: Securing ad hoc networks in extreme emergency cases. In: Proceedings of the World Wireless Research Forum, Paris (2009)
3. Kannhavong, B.: A survey of routing attacks in mobile ad hoc networks. IEEE Wirel. Commun. **5**, 85–91 (2007)
4. Maheshwari, R.; Gao, J.; Das, S.R.: Detecting wormhole attacks in wireless networks using connectivity information. In: 26th IEEE International Conference on Computer Communications, pp. 107–115 (2007)
5. Lemon, J.: Resisting SYN flood DoS attacks with a SYN cache. In: Proceedings of The BSD Con Conference, pp. 89–97. San Francisco (2002)
6. Bin, X.; Chen, W.; He, Y.X.; Sha, E.H.-M.: An active detecting method against SYN flooding attack. In: Proceedings of 11th International Conference on Parallel and Distributed Systems, pp. 709–715 (2005)
7. Bin, X.; Wei, C.; Yang Xiang, H.: An autonomous defence against SYN flooding attacks: detect and throttle attacks at the victim side. J. Parallel Distrib. Comput. **68**(4), 456–470 (2008)
8. Siris Vasilios, A.; Fotini, P.: Application of anomaly detection algorithms for detecting SYN flooding attacks. Comput. Commun. **29.9**, 1433–1442 (2006)
9. Wang, S.; Sun, Q.; Zou, H.; Yang, F.: Detecting SYN flooding attacks based on traffic prediction. Secur. Commun. Netw. **5**, 1131–1140 (2012)
10. Haris, S.H.C.; Ahmad, R.B.; Ghani, M.A.H.A.: Detecting TCP SYN flood attack based on anomaly detection. In: Second International Conference on Network Applications Protocols and Services, pp. 240–244 (2010)
11. Salem, O.; Mehaoua, A.; Vaton, S.; Gravey, A.: Flooding attacks detection and victim identification over high speed networks. In: Information Infrastructure Symposium, pp. 1–8 (2009)
12. Tartakovsky, A.G.; Polunchenko, A.S.; Sokolov, G.: Efficient computer network anomaly detection by changepoint detection methods. IEEE J. Sel. Top. Signal Process. **7**(1), 4–11 (2013)
13. Changhua, S.; Jindou, F.; Lei, S.; Bin, L.: A novel router-based scheme to mitigate SYN flooding DDoS attacks. In: Proceedings of the IEEE INFOCOM (2007)
14. Chen, W.; Dit-Yan, Y.: Defending against TCP SYN flooding attacks under different types of IP spoofing. In: Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL), pp. 38–38 (2006)

15. Changhua, S.; Hu, C.; Tang, Y.; Liu, B.: More accurate and fast SYN flood detection. In: Proceedings of 18th International Conference on Computer Communications and Networks, pp. 1–6 (2009)
16. Ling, Y.; Ye, G.; Guiyi, W.: Detect SYN Flooding Attack in Edge Routers. Int. J. Secur. Appl. **3**, 31–45 (2009)
17. Kim, T.; Choi, Y.; Kim, J.; Hong, S.J.: Annulling SYN flooding attacks with whitelist. In: Proceedings of the IEEE 22nd International Conference on Advanced Information Networking and Applications, pp. 371–376 (2008)
18. Dinil, M.D.; Murthy, H.A.; Gonsalves, T.A.: Detection of SYN flooding attacks using linear prediction analysis. In: 14th IEEE International Conference on Networks, pp. 218–223 (2006)
19. Korczynski, M.; Janowski, L.; Duda, A.: An accurate sampling scheme for detecting SYN flooding attacks and portscans. In: Proceedings of the IEEE International Conference on Communication, pp. 1–5 (2011)
20. Ranjan, N.; Murthy, H.A.; Gonsalves, T.A.: Detection of SYN flooding attacks using generalized autoregressive conditional heteroskedasticity (GARCH) modeling technique. In: Proceedings of the 2010 National Conference on in Communications, pp. 1–5 (2010)
21. Ohsita, Y.; Shingo, A.T.A.; Murata, M.: Detecting distributed Denial-of-service attacks by analyzing TCP SYN packets statistically. IEICE Trans. Commun. 2868–2877 (2006)
22. Wang, H.; Zhang, D.; Shin, K.: Detecting SYN flooding attacks. In: Proceedings of IEEE INFOCOM, pp. 1530–1539 (2002)
23. Bellaiche, M.; Gregoire, J.-C.: SYN flooding attack detection based on entropy computing. In: IEEE Proceedings of the Global Telecommunications Conference, pp. 1–6 (2009)
24. Changhua, S.; Jindou, F.; Bin, L.: A robust scheme to detect SYN flooding attacks. In: Second International Conference on Communications and Networking, pp. 397–401 (2007)
25. Al-Duwairi, B.; Manimaran, G.: Intentional dropping: a novel scheme for SYN flooding mitigation. In: Proceedings of INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies, pp. 2820–2824 (2005)
26. Mirkovic, J.; Reiher, P.: D-WARD: a source-end defense against flooding denial-of-service attacks. IEEE Trans. Dependable Secure Comput. 216–232 (2005)
27. Garg, A.; Reddy, A.N.: Mitigation of DoS attacks through QoS regulation. Microprocess. Microsyst. **28**(10), 521–530 (2004)
28. Haggerty, J.; Berry, T.; Shi, Q.; Merabti, M.: DiDDeM: a system for early detection of TCP SYN flood attacks. In: IEEE Proceddings of the Global Telecommunications Conference, pp. 2037–2042 (2004)
29. Schuba, C.L.; Krsul, I.V.; Kuhn, M.G.; Spafford, E.H.; Sundaram, A.; Zamboni, D.: Analysis of a denial of service attack on TCP. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 208–223 (1997)
30. Von Neumann, J.; Morgenstern, O.: Theory of Games and Economic Behavior (60th Anniversary Commemorative Edition). Princeton university press, Princeton (2007)
31. Osborne, M.; Rubinstein, A. (1994) A Course in Game Theory. The MIT press, Cambridge
32. Agah, A.; Das, S.K.; Basu, K.; Asadi, M.: Intrusion detection in sensor networks: A non-cooperative game approach. In: Proceedings of the Network Computing and Applications, pp. 343–346 (2004)
33. Agah, A.; Basu, K.; Das, S.K.: Preventing DoS attack in sensor networks: a game theoretic approach. In: Int. Conf. Commun. 3218–3222 (2005)
34. Panaousis, E.A.; Politis, C.: Non-cooperative games between legitimate nodes and malicious coalitions in MANETs. In: proceedings of the Future Network and Mobile Summit Conference (2011)
35. Panaousis, E.; Politis, C.: A game theoretic approach for securing AODV in emergency mobile ad hoc networks. In: Proceedings of the 34th IEEE Conference on Local Computer Networks, pp. 985–992 (2009)
36. Anantvalee, T.; Wu, J.: A survey on intrusion detection in mobile ad hoc networks. In: Wireless Network Security, pp. 159–180. Springer, US (2007)
37. Murthy, C.S.R.; Manoj, B.S.: Ad hoc wireless networks: architectures and protocols. Pearson Education (2004)