DOI: 10.21917/ijct.2020.0339

HYBRID NODE WATCHING TECHNIQUE BASED DOS FLOODING ATTACK DETECTION IN WIRELESS SENSOR NETWORK

L. Sheeba and V.S. Meenakshi
Department of Computer Applications, PSGR Krishnammal College for Women, India
Department of Computer Science, Chikkaana Government Arts College, India

Abstract

Intrusion detection is the most concentrated research issue in the wireless sensor network where presence of intrusion activities are most difficult to find where there is no centralized architecture to monitor. One of the most frequently found intrusion activities in wireless sensor network are Denial of Service (DoS) Flooding attacks. DoS flood attacks would send large volume of chunk messages to the end node in order to corrupt the functioning of the particular node. Some of the most important DoS flooding attacks that are found in the network are ICMP flood attack, Synchronous Flood attack, UDP Flood attack, and Web attacks. All these networks would send enormous amount of messages such internet control message packets, synchronous messages, UDO messages correspondingly to the web servers to collapse the normal functioning of them by consuming energy resources and so on. In the previous research works, Sybil attacks and DDoS attacks are detected and avoided by introducing the method namely Privacy Concerned Anonymous Authentication Method (PAAM). However these research methods reduced in its attack detection rate with the presence of DoS Flooding attacks. This is focused and resolved in this work by introducing a method namely Hybrid Node Watching Technique (HNWT). This research technique attempt to find the variation in the data's and control messages transmitted between the end nodes to find the flooding attack presence. This is done through the trust nodes which are selected optimally by using cat swarm algorithm. These optimally selected nodes will monitor data transmission behaviour to predict malicious node presence. The overall implementation of this research work is done in NS2 simulation environment from which it is proved that proposed research technique tends to have increased attack detection rate.

Keywords:

Intrusion Attacks, DoS Flooding Attacks, Node Monitoring, ICMP Flood Attacks, Syn Flood Attack, UDP Flood Attack, Web Attacks

1. INTRODUCTION

H. Most ascending as well as demanding area of research in recent days is wireless sensor networking. A collection of autonomous nodes forms a Wireless Sensor Network (WSN). With small frequency and bandwidth consumption in wireless channel, they transmit a data [1]. For various applications like military applications, scientific examination, data collection monitoring, wireless sensor networks gives a low cost solutions, which makes them as a most popular one [2]. In network, every node can find its neighbouring nodes and in collection, for forming routes, these data can be used. Wireless Sensor Networks are most commonly vulnerable to Denial of Service attacks due to some weakness like broadcast transmission medium, limited processing capability and memory [3]. The WSN's capability are reduced due to this kind of attacks and it makes the lifetime of a WSN as a smaller one. In network, consumption resources are affected by this very often and energy consumption is enhanced and throughput is minimized [4].

A type of attack which restricts the users to utilize some specific network resources is called Denial of Service (DoS) attack and the resource may include entire system and/or website [5].A synchronized attack called Distributed Denial of Service (DDoS) attack, which is performed on some specific network's available services via compromised computing systems, which makes tracking of this DDoS control packets as a highly difficult one [6]. A type of Denial of Service (DoS) type of attack is flooding attack. The vital problem of flooding attack is that the flooder node is flooding the full network [7]. The flooding attack is where attacker generates route request messages and floods request simply by not even monitoring routing table for route. Once legitimate node receives RREQ, nodes in-between in their routing table will attempt to focus on destination route and eventually flood request to their respective neighbors as nodes have a route to destination.

The flooding attack's major objective is to take power by consuming a huge amount of battery and network bandwidth [8]. It will ultimately lead to small number of network performance - related issues. Flooding attack results in a breakdown in terms of output, battery power exhaustion and bandwidth inefficiency. AODV routing protocol is vulnerable to malicious attacks due its flexibility (on demand) in route discovery method. Due to the on-demand path discovery nature of AODV, it uses various metrics such as RREQ packets. A malicious node easily changes the contents of these packets to launch the attack. The AODV motivates WSN nodes to quickly acquire routes for new destinations, which do not need nodes to keep routes to non - networked destinations. RREQ message is the message that is sent to sink from the source to connect and send data to sink from the source

Major objective of this research work is for protecting Wireless Sensor Network from a type of DoS attack called flooding. All network resources like computing power, energy and bandwidth may be exhausted by folding. A new detection technique called early detection of DoS attack via distributed technique is proposed in this work. According to the transmission count based on neighbouring node's count, attackers are identified in this scheme. A threshold value is used in this scheme for comparing transmissions and other node's PDR in network.

2. RELATED WORKS

Hassanzadeh et al. [9] proposed an efficient flooding with neighborhood keys in WSN secured. The research paper involves checking whether a flooding packet can achieve 100% network coverage when every node clearly selects one of its keys to unicast the message. It results in NP - hard, proposing an application development version of it, and implementing a MAX-SFN approximation algorithm. It exhibits the 100 percent network

coverage that can be achieved by flooding packets at low cost through simulations.

Moon et al. [10] proposed the overall consequences of RREQ flooding attacks on different network performance constrains such as initiated route request packets, energy consumption, buffer overflow, end-to-end delay and throughput was studied. RREQ flooding attack decreases the WSN's performance because it drains the network's restricted resources quickly. Throughout this analysis helps to design relevant mechanisms of security to thwart RREQ flooding attack.

Bhalodiya et al. [11] proposed a system finding number of devious network nodes and dropping entirely fake packets. This paper provided a flood attack solution using RREQ flood attack. The results of the simulation are accomplished using parameters like packet delivery ratio, end-to-end-delay and throughput. This solution can be used to recognize and eliminate any number of MANET malicious nodes and to locate a safer route from source to destination by redirecting malicious nodes. The concern will be on analyzing the attack issue in further protocols in the future.

Prusty et al. [12] proposed few interesting concepts and explains the concepts of wireless sensor networks, challenges, different security threats, network attacks, classification of attacks and countermeasures. This will generate interest in imagining new ideas for a reliable, robust and safer wireless sensor network among future researchers.

Rolla et al. [13] proposed a review on several techniques for protecting DDoS attack. It is carried out by a brief explanation about the wireless sensor network and DDOS attack. Various prevention techniques for DoS attack are reviewed and a comparative analysis of different techniques tabularly designed.

Ping et al. [14] proposed the flooding Attack of ad hoc routing protocols on demand. The detailed view of ad-hoc flood attack and AODV routing protocols has been elaborated. There is a tabulated comparison of Ad hoc Flooding Attack and SYN Flooding Attack. In order to resist this attack, Flooding Attack Prevention (FAP) is designed to develop an algorithm using a neighbor suppression method. The results of the implementation show that the FAP is effectively defending the Ad hoc Flooding Attack with a slight overload.

Chouhan et al. [15] proposed effective way to identify and prevent the flooding attack. The efficient way of using AODV protocol to prevent flooding attack is analyzed. In order to combine efficient secure routing algorithms into the network, MANETs requires a brief understanding and structuring of the security attacks. An algorithm is developed for RREQ flooding attack. Further this study can be enhanced optimizing value of threshold and improving their performance.

Shandilya et al. [16] proposed a distributive approach for detecting and preventing RREQ flooding. The effectiveness depends on the threshold values being selected. Together with the trust estimation function, the DSR routing protocol is used. The delay queue approach minimizes the node's chance of accidental blacklisting, But the detection of malicious nodes is also delayed by permitting them to forward more packets once slowdown queue time - out arises.

3. HYBRID NODE WATCHING TECHNIQUE FOR DOS FLOODING ATTACK DETECTION

This research technique attempt to find the variation in the data's and control messages transmitted between the end nodes to find the flooding attack presence. This is done through the trust nodes which are selected optimally by using cat swarm algorithm. These optimally selected nodes will monitor data transmission behaviour to predict malicious node presence.

3.1 OPTIMAL MONITORING NODE SELECTION BASED ON TRUST VALUE

Monitoring node plays an important role in intrusion detection framework. The monitoring nodes is to monitor ongoing data transmission and will detect any sudden variation or differences in the transmitted data. Thus monitoring nodes can detect the presence of DoS flood attacks. These monitoring nodes should be enough resource availability and trustable which is responsible for detecting the DoS flooding attacks. In this work, monitoring node is selected optimally using Cat Swarm Optimization algorithm under consideration of objective termed as trust level of nodes.

In the world of swarm intelligence, CSO is a modern optimization algorithm. The CSO algorithm has been found to achieve solutions more easily with the problem of convergence resolved. The algorithm for CSO is smoother than other algorithms. It can overcome the global optimization problem than other approaches. The CSO algorithm models cats' behaviour (nodes) in two modes: Search mode and Trace mode. The swarm is made up of an initial population of particles to be searched in the space of the solution. For example, it can simulate birds, ants and bees and, respectively, build optimization of particle swarm, optimization of ant colony and optimization of bee colony.

Here it uses cats as particles to solve the problems in CSO. Every cat has its own location in CSO, consisting of D dimensions, speeds for each dimension, a fitness value that reflects the cat's accommodation to the fitness function, and a flag to decide if the cat is in search mode or tracing mode. The optimum location of one of the cats will be the final solution. The optimal solution is retained by the CSO until it approaches the end of the iterations. In order to solve the problems described below the CSO algorithm has two methods:

3.1.1 Seeking Mode:

Seeking mode is used to model cats' behavior in resting time and being-alert time. This mode is used to think and decide about next move. There are four major parameters in this mode namely, self-position consideration (SPC), counts of dimension to change (CDC), seeking range of the selected dimension (SRD) and seeking memory pool (SMP). Following describes seeking mode's process.

Step 1: Make j copies of cat k's present position, where j = SMP. If SPC value is true, let j = (SMP-1), then retain present position as one of the candidates.

Step 2: For every copy, based on CDC, randomly plus or minus SRD percent present values and replace old ones.

Step 3: All candidate point's fitness values (FS) is computed.

Step 4: If all FS are not exactly equal, every candidate points selecting probability is computed using Eq.(1), otherwise every candidate points selecting probability is set as 1.

Step 5: Randomly pick the point to move to from candidate points, and replace cat *k*'s position.

$$P_i = |SSE_i\text{-}SSE_{max}|/(SSE_{max}\text{-}SSE_{min}) \quad (1)$$

If fitness function's objective is to compute minimum solution, $FS_b = FS_{max}$, otherwise $FS_b = FS_{min}$.

3.1.2 Tracing mode:

In this algorithm, tracing mode is a second one. Foods and targets are traced by cats in this mode. Tracing process is described mentioned below.

Step 1: Using Eq.(2), for every dimension, velocity is updated..

Step 2: Check if velocities are in maximum velocity range. In case, new velocity is over range, it is set equal to limit.

$$V_{k,d} = V_{k,d} + r_1c_1(X_{best,d}\text{-}X_{k,d}) \quad (2)$$

Step 3: Based on Eq.(3), cat_k position is updated

$$X_{k,d} = X_{k,d} + V_{k,d} \quad (3)$$

Cat's which has a better fitness value's position is given by $X_{best,d}$, cat *k*'s position is expressed as $X_{k,d}$, acceleration coefficient is expressed as c_1 and it is used to extend cat's velocity for moving in solution space and in general, its value will be 2.05 and a random value is represented as r_1 and it has uniform generation with the values between 0 to 1.

For combining two modes into this algorithm, mixture ratio (MR) is defined, which indicates mixing rate of tracing mode and seeking mode. Cats count that are moved into seeking mode process is decided using this parameter. For instance, with a population size of 50 and MR of 0.7, there will be 50×0.7=35 cats movement into seeking mode and remaining 15 cats will be moved into tracing mode in this iteration.

The CSO algorithm is summarized as, first *N* cats (nodes) are crated and flags, velocities, positions (location) of cats are initialized (*). Every cats fitness value are computed based on fitness function namely, delay, bandwidth and energy. Best cat is maintained in memory (X_{best}). In next step, cats are applied into seeking or tracing mode based on cat's flag. Cats count are re-computed after completing related process and based on MR parameter, cats are set into tracing or seeking mode. At last, termination condition is checked. Program is terminated, if it is satisfied. Else go to (*). From network environment, highly optimal monitoring nodes can be selected using this algorithm via monitoring data transmission. Monitoring node's optimum selection can be done using this proposed research technique and it can communicate with every nodes in the environment.

3.1.3 Trust Level Estimation:

Over a specific range (-1 to +1), trust may be represented using a continuous variable and it also may be represented using a values with labels like very high trust, high trust, medium trust and low trust. In order to make a trusted communication, requested node's trust values are computed by node in the network, if it receives communication request from other nodes in network. This value is termed as node's indirect trust value. It is also termed as node's initial trust value. Node started to communicate, if this initial trust value of node is sufficient. In other cases, direct trust value computation is performed by nodes. As like in trust framework, three models are involved in direct trust computation. They are, node's reliability model, node's mobility model and node's security model.

Algorithm: To compute node's Trust

Initial condition: Node wants to communicate with other node in network.

Input: Reliability, Security, Node id, Node's Mobility Model.

Output: Trust value calculation and communication.

Begin:

Node's initial trust computation:

$T_{initial} = (S+U)/(T_i+S)$ or P_r;

If ($T_{initial}$ is sufficient to communicate)

Allow communication with node.

Else for node's security model trust value is computed.

$T_s=A+E+R$;

If (T_s is sufficient to communicate)

Then allow communication with node.

Else for node's mobility model

Trust value is computed.

End

If node is static

Then assume node's trust value in mobility model is zero.

Else mobility node's trust value is computed.

$T_m=M_e+E_m$;

End

If (T_m is sufficient to communicate)

Then allow communication with node.

Else for node's reliability model trust value is computed.

$T_r = D+E_d$;

If (T_r is sufficient to communicate)

Then allow communication;

Else calculate the overall trust for node.

Overall trust = $T_{initial}+T_s+T_m+T_r$;

End

If Overall trust is sufficient to communicate

Then allow communication with node.

Else

Deny communication with node.

End

End

3.2 HYBRID WATCHING TECHNIQUE FOR DOS FLOODING ATTACK DETECTION

For saving its own resources, packet forwarding are denied by selfish nodes. This characteristics indicates that selfish node neither involves in routing nor relays data packets. Unallowable packet drops are produced due to this characteristics of selfish node. This characteristics of selfish node are produced because of adversaries executing packet drop attacks or because of internal conflicts like node failures and overload. In those conditions,

secured packet transmission are not provided by paths constructed using selfish nodes.

In Side Channel Monitoring (SCM) approach, a centralized contact based watchdog is employed for monitoring misbehaviour of routing nodes. This watchdog node collects information about every node in its neighbourhood which are comparatively analysed with normal node's behaviour. If packet transmission behaviour of nodes seems abnormal, watch dog initiates warning message to source node. The packet transmission i.e. variation in received packets count and packets forwarding count is monitored while exception cases (new nodes forwarding control messages to find neighbouring nodes) are considered.

A list of data packet IDs which are yet to be receive a TWOACK acknowledgment packet from a node two hops away is maintained by data packets sender or router for detecting misbehaviour. For every forwarding link, a unique list is maintained by every node. For routing path, suppose if R1 do not know whether R3 receives packet or not. This is avoided by TWO-ACK scheme where R3 will send TWOACK packet back to source node through path R2-R1. Thus R1 can know whether packets are received by R3 or not. Now if R3 is a selfish node performing drop attacks, an ERROR message is sent to source. It can be said that genuine route failures also results in similar behaviour. But in TWOACK, genuine route failures initiates' voluntary ERROR message which is entirely different from malicious behaviours as genuine route failures may take place due to mobility or excessive traffic in forwarding node's vicinity.

Algorithm 2: Hybrid Node Watching Technique

Initialise: Source node *S* and Destination node *D*

S generates Route path ID list

Set time threshold *thres*

S Sends data packets *p* to *D* through routing path *S*-*R*1-*R*2-*R*3-*D*

When *R*3 receives *p*, it sends TWOACK with sequence number to *S*

S analyzes TWOACK packets

If two packs have same sequence number, then

S initiates *R*3 as selfish node behavior

Else

Remove *R*3 node ID from path ID list

End if

If (time *t*=*thres*)

Analyze route path ID list

If packet *p* from *R*3 has (*t*>*thres*)

Call watchdog *C* by sending REQ packets with *R*3 node ID

C monitors packet transmission of *R*3

If (*t*>*thres*) is satisfied

*R*3 is confirmed as malicious node

Else

Perform transmission process

End if

The hybrid approach initializes the source and destination nodes and forms the routing path. Every node's ID in path is stored in path ID list managed by source node. Similarly each successive node maintains a list for maintaining path information. Each node, on receiving data packets, sends TWOACK packets to the source through preceding nodes. On receiving the TWOACK packets, the source node analyzes the ACK. If two nodes send packets with same sequence number, it confirms the selfish behavior while if it is not, the particular node ID is removed from path ID list. Then the path ID list is analyzed from which the packets with time greater than thresholds are detected. Then the watchdog is called to monitor the particular node. When monitoring, if the threshold status is again the same, the node is deemed as selfish node and it is removed from the route. Thus the proposed approach enhances the security in packet transmission.

4. RESULTS AND DISCUSSION

The proposed HNWT's performance is evaluated in this section using NS-2 simulator. In this network simulation environment, within a 100×100 meters area, 100 nodes are randomly placed. In simulation, nodes are classified into two classes namely, malicious nodes and well-behaved nodes. In simulated scenarios, DOS flooding attacks are launched by malicious nodes. The proposed HNWT system is compared with available systems like LEoNIDS, Attack Feature based Fast and Accurate Intrusion Detection System (AF-FAIDS), Prioritization Based Delay Avoided Secured and Reliable Data Transmission Method (PBDASRDT), Latency and Power aware Reliable Intrusion Detection System (LP-RIDS) and PAAM in order to evaluate the performance of it. The Table.1 summarizes the parameters used to evaluate the trust system in this research work. Following metrics like DoS flooding attack probability, success rate, false positive rate and false alarm rate are used for evaluating the proposed HNWT model.

Table.1. Simulation parameters

Simulation Parameters	Values
Channel	Wireless Channel
Mac	802.11
Antenna class	Omni antenna
Routing Protocol	AODV
Initial Energy	100 joules
Traffic class	CBR
Agent	UDP
Area of simulation	100×100 meters
Node's count	100

- ***False Alarm Rate*:** In general, false alarm ratio is abbreviated as FAR, and it is a false alarm's count per total number of warnings or alarms attack detection.
- ***False Positive Rate*:** Ratio between negative events count which are categorized wrongly as positive to total actual negative events count irrespective of classification defines false positive rate. It gives the percentage that shows incorrect identification of attacker nodes by our algorithm.
- ***Success Rate vs. Number of Attacker Node*:** Success rate, which is a percentage that our algorithm can correctly identify attacker nodes.

- ***Successful Attack Detection Probability*:** Attack probability is defined as the effectiveness of proposed algorithm to capture the present of attacks from the total number of attacks. That is, it is a ratio between captured attack's count to total attacks present in environment.

4.1 PERFORMANCE ANALYSIS OF ICMP FLOODING ATTACK

In this section, comparison analysis of attack detection process with the presence of ICMP flooding attacks is shown. In the Fig.1, false alarm rate comparison is shown against different number of attacker nodes presence in the environment.

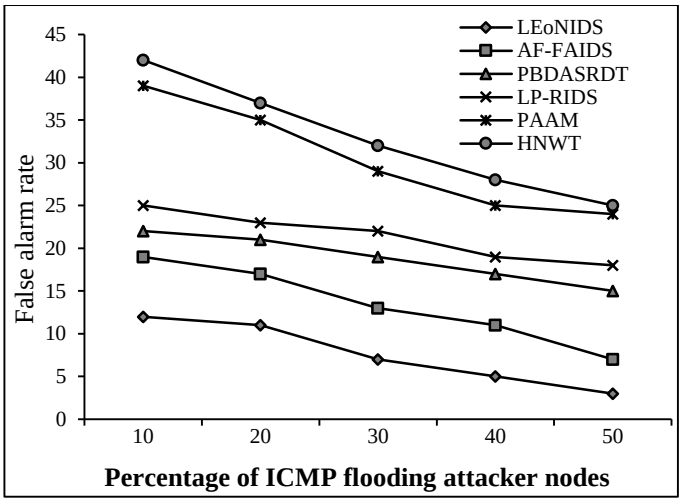

Fig.1. False alarm rate vs number of attacker nodes

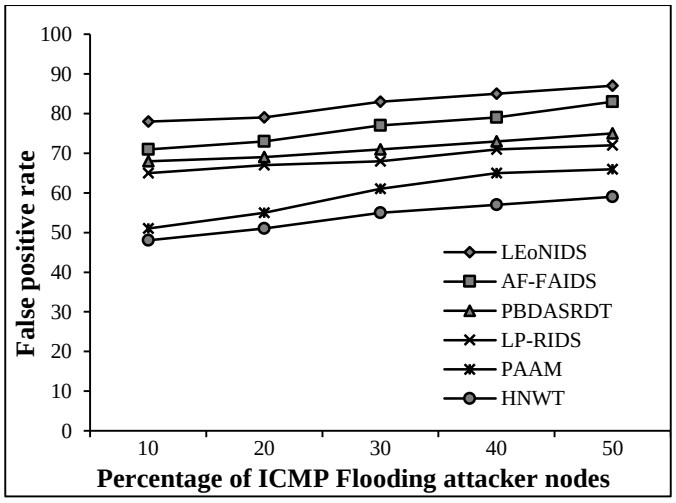

Fig.2. False positive rate vs percentage of attacker nodes

In Fig.1, comparison evaluation of the false alarm rate for the proposed and existing methodologies are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with higher detection of attacker nodes. From this comparison it is proved that proposed HNWT shows 2.4% higher false alarm rate than PAAM, 11.4% higher alarm rate than LP-RIDS, 14% higher false alarm rate than PBDASRDT, 19.4% higher false alarm rate than AF-FAIDS and 25.2% higher false alarm rate than LEoNIDS.

In Fig.2, comparison evaluation of the false positive rate for the proposed and existing methodologies are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with lesser wrong detection of attacker nodes. From this Fig.it is proved that the HNWT shows 5.6% lesser false positive rate than PAAM, 14.6% lesser false positive rate than LP-RIDS, 17.2% lesser false positive rate than PBDASRDT, 22.6% lesser false positive rate than AF-FAIDS and 28.4% lesser false positive rate than LEoNIDS.

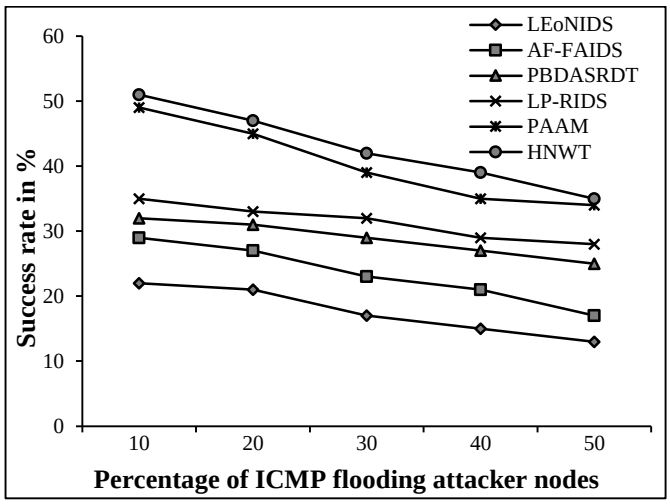

Fig.3. Success rate comparison

In Fig.3, comparison evaluation of the success rate for the proposed and existing methodologies are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with accurate detection of attacker nodes. From this comparison, it is proved that proposed HNWT shows 2.4% higher success rate than PAAM, 11.4% higher success rate than LP-RIDS, 14% higher success rate than PBDASRDT, 19.4% higher success rate than AF-FAIDS and 25.2% higher success rate than LEoNIDS.

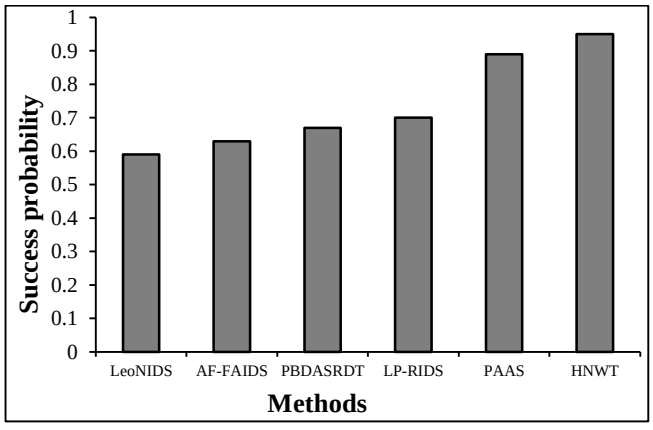

Fig.4. Flooding attack probability comparison

In Fig.4, comparison evaluation of the success probability for the proposed and existing methodologies is given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with accurate detection of attacker nodes. From this comparison it is proved that proposed HNWT shows 6.74% higher attack

detection probability than PAAS, 35.71% higher attack detection probability than LP-RIDS, 41.79% higher attack detection probability than PBDASRDT, 50.79% higher attack detection probability than AF-FAIDS and 61.01% higher attack detection probability than LEoNIDS.

4.2 PERFORMANCE ANALYSIS OF SYNCHRONOUS FLOODING ATTACK

In this section, comparison analysis of attack detection process with the presence of synchronous flooding attacks is shown. In the Fig.5, false alarm rate comparison is shown against different number of attacker nodes presence in the environment.

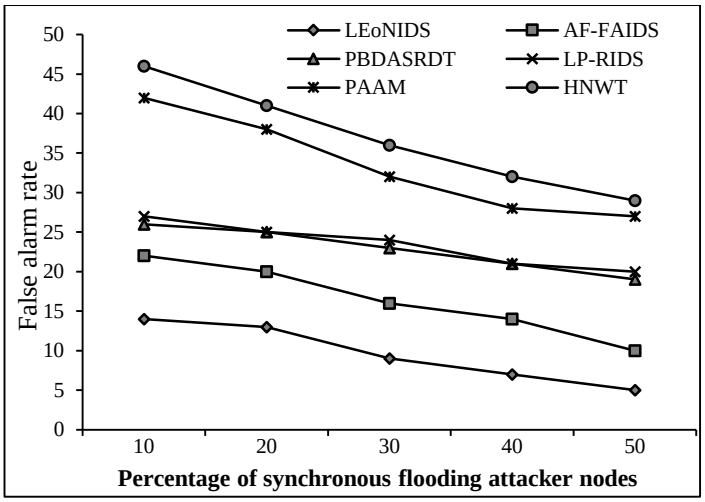

Fig.5. False alarm rate vs number of attacker nodes

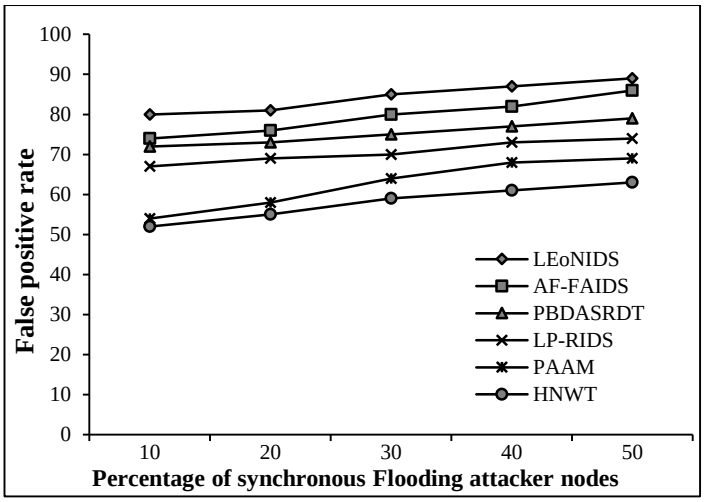

Fig.6. False positive rate vs percentage of attacker nodes

In Fig.5, comparison evaluation of false alarm rate for the proposed and available techniques are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with higher detection of attacker nodes. From this comparison it is proved that proposed HNWT shows 3.4% higher false alarm rate than PAAM, 13.4% higher alarm rate than LP-RIDS, 14% higher false alarm rate than PBDASRDT, 20.4% higher false alarm rate than AF-FAIDS and 27.2% higher false alarm rate than LEoNIDS.

In Fig.6, comparison evaluation of the false positive rate for the proposed and existing methodologies are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with lesser wrong detection of attacker nodes. From this Fig.it is proved that HNWT shows 4.6% lesser false positive rate than PAAM, 12.6% lesser false positive rate than LP-RIDS, 17.2% lesser false positive rate than PBDASRDT, 21.6% lesser false positive rate than AF-FAIDS and 26.4% lesser false positive rate than LEoNIDS.

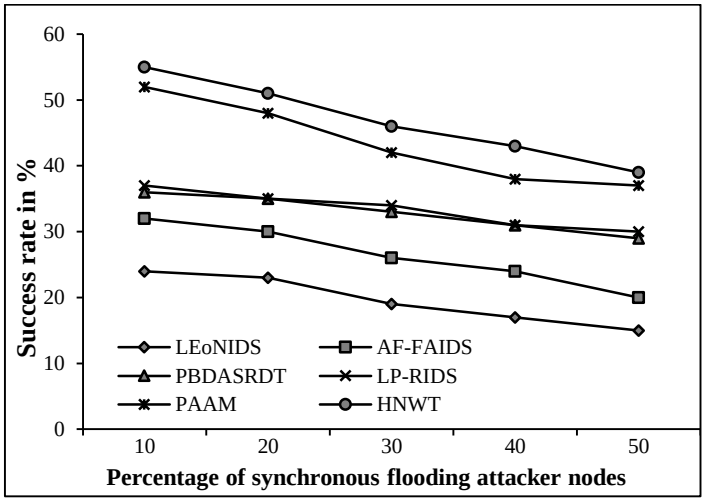

Fig.7. Success rate comparison

In Fig.7, comparison evaluation of the success rate for the proposed and existing methodologies are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with accurate detection of attacker nodes. From this comparison, it is proved that proposed HNWT shows 3.4% higher success rate than PAAM, 13.4% higher success rate than LP-RIDS, 14% higher success rate than PBDASRDT, 20.4% higher success rate than AF-FAIDS and 27.2% higher success rate than LEoNIDS.

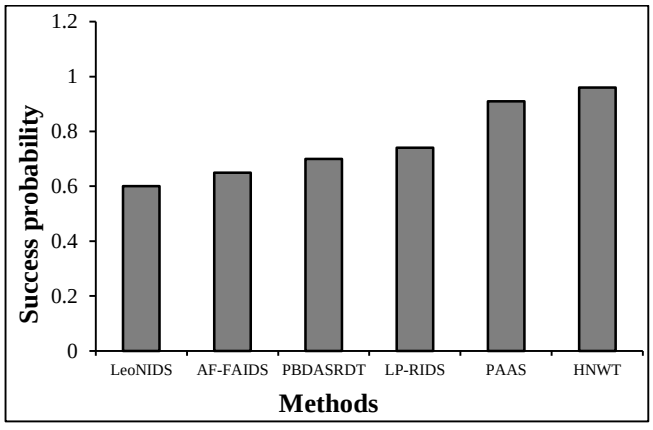

Fig.8. Flooding attack probability comparison

In Fig.8, comparison evaluation of the success probability for the proposed and existing methodologies is given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with accurate detection of attacker nodes. From this comparison it is proved that proposed HNWT shows 5.49% higher attack

detection probability than PAAS, 29.72% higher attack detection probability than LP-RIDS, 37.14% higher attack detection probability than PBDASRDT, 47.69% higher attack detection probability than AF-FAIDS and 60% higher attack detection probability than LEoNIDS.

4.3 PERFORMANCE ANALYSIS OF UDP FLOODING ATTACK

In this section, comparison analysis of attack detection process with the presence of UDP flooding attacks is shown. In the Fig.9, false alarm rate comparison is shown against different number of attacker nodes presence in the environment.

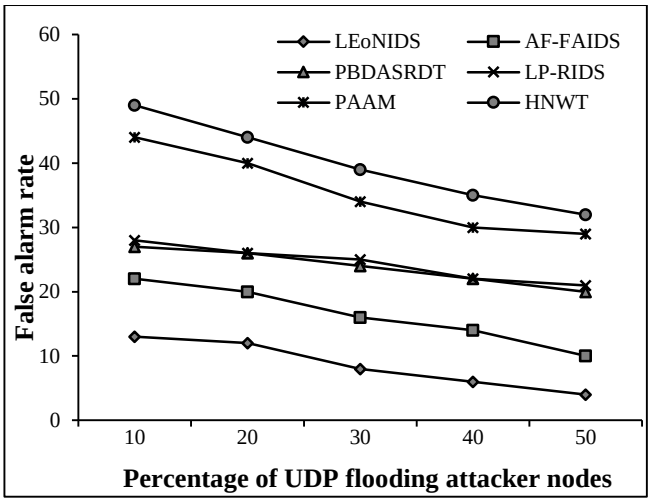

Fig.9. False alarm rate vs number of attacker nodes

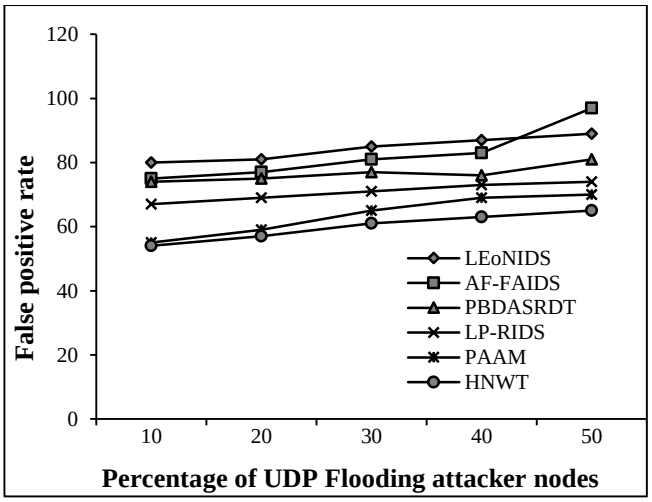

Fig.10. False positive rate vs percentage of attacker nodes

In Fig.9, comparison evaluation of false alarm rate for proposed and available methodologies are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with higher detection of attacker nodes. From this comparison it is proved that proposed HNWT shows 4.4% higher false alarm rate than PAAM, 15.4% higher alarm rate than LP-RIDS, 16% higher false alarm rate than PBDASRDT, 23.4% higher false alarm rate than AF-FAIDS and 31.2% higher false alarm rate than LEoNIDS.

In Fig.10, comparison evaluation of the false positive rate for the proposed and existing methodologies are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with lesser wrong detection of attacker nodes. From this Fig.it is proved that the HNWT shows 3.6% lesser false positive rate than PAAM, 10.8% lesser false positive rate than LP-RIDS, 16.6% lesser false positive rate than PBDASRDT, 22.6% lesser false positive rate than AF-FAIDS and 24.4% lesser false positive rate than LEoNIDS.

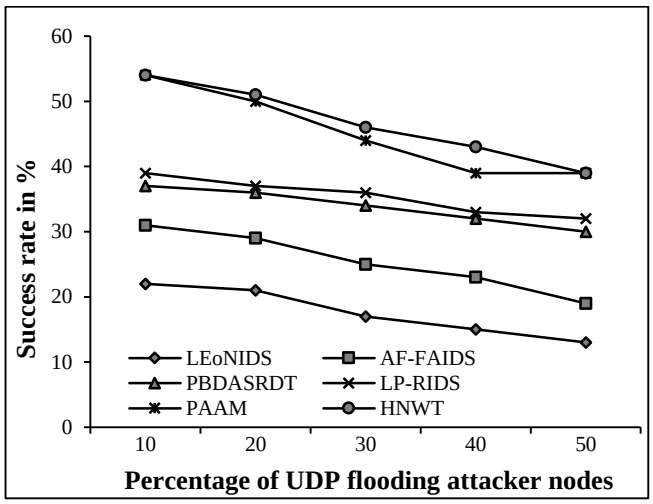

Fig.11. Success rate comparison

In Fig.11, comparison evaluation of the success rate for the proposed and existing methodologies are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with accurate detection of attacker nodes. From this comparison, it is proved that proposed HNWT shows 1.4% higher success rate than PAAM, 11.2% higher success rate than LP-RIDS, 12.8% higher success rate than PBDASRDT, 21.2% higher success rate than AF-FAIDS and 29% higher success rate than LEoNIDS.

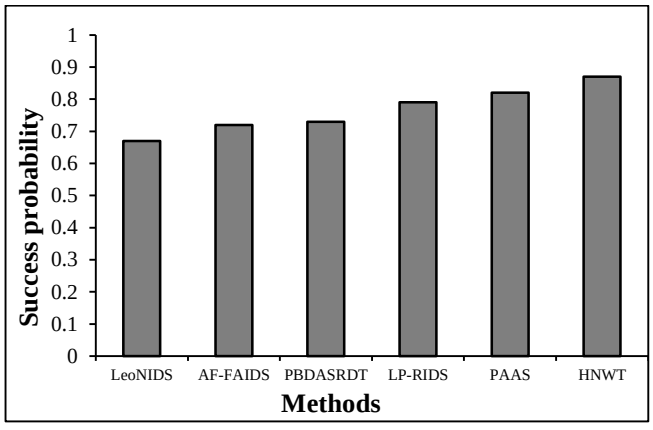

Fig.12. Flooding attack probability comparison

In Fig.12, comparison evaluation of the success probability for the proposed and existing methodologies is given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with accurate detection of attacker nodes. From this comparison it is proved that proposed HNWT shows 6.09% higher attack

detection probability than PAAS, 10.12% higher attack detection probability than LP-RIDS, 19.17% higher attack detection probability than PBDASRDT, 20.83% higher attack detection probability than AF-FAIDS and 29.85% higher attack detection probability than LEoNIDS.

4.4 PERFORMANCE ANALYSIS OF WEB ATTACK

In this section, comparison analysis of attack detection process with the presence of Web attacks is shown. In Fig.13, the false alarm rate comparison is shown against different number of attacker nodes presence in the environment.

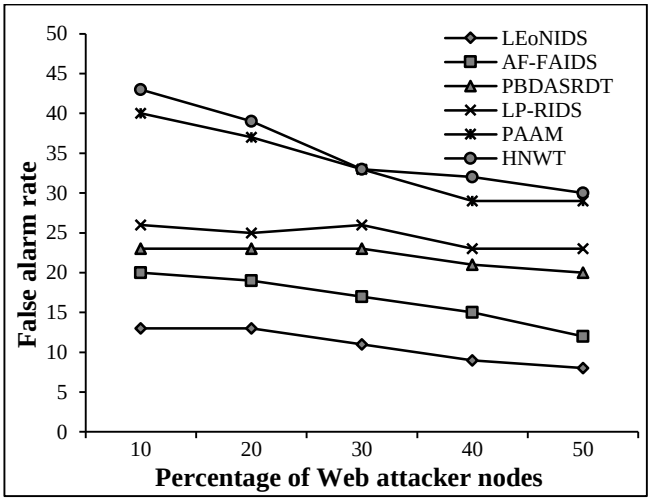

Fig.13. False alarm rate vs number of attacker nodes

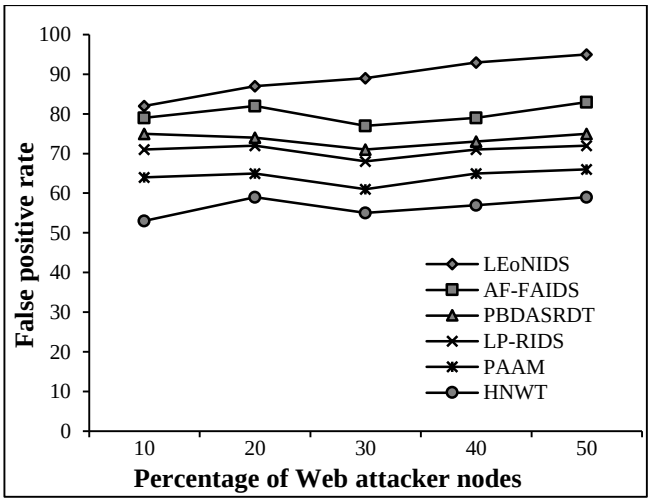

Fig.14. False positive rate vs percentage of attacker nodes

In Fig.13, comparison evaluation of false alarm rate for proposed and available techniques are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than the previous methodologies with higher detection of attacker nodes. From this comparison it is proved that proposed HNWT shows 1.8% higher false alarm rate than PAAM, 10.8% higher alarm rate than LP-RIDS, 13.4% higher false alarm rate than PBDASRDT, 18.8% higher false alarm rate than AF-FAIDS and 24.6% higher false alarm rate than LEoNIDS.

In Fig.14, comparison evaluation of the false positive rate for the proposed and existing methodologies are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than the previous methodologies with lesser wrong detection of attacker nodes. From this Fig.it is proved that the HNWT shows 7.6% lesser false positive rate than PAAM, 14.2% lesser false positive rate than LP-RIDS, 17% lesser false positive rate than PBDASRDT, 23.4% lesser false positive rate than AF-FAIDS and 32.6% lesser false positive rate than LEoNIDS.

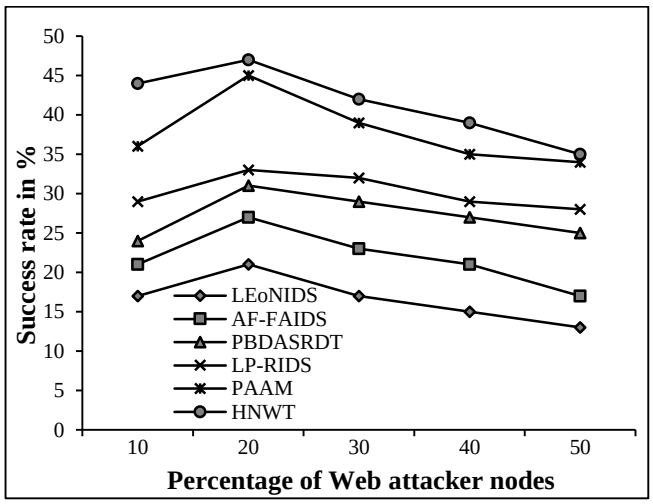

Fig.15. Success rate comparison

In Fig.15, comparison evaluation of the success rate for the proposed and existing methodologies are given. From this comparison, it indicates that proposed method HNWT tends to have better performance than previous methodologies with accurate detection of attacker nodes. From this comparison, it is proved that proposed HNWT shows 3.6% higher success rate than PAAM, 11.2% higher success rate than LP-RIDS, 14.2% higher success rate than PBDASRDT, 19.6% higher success rate than AF-FAIDS and 24.8% higher success rate than LEoNIDS.

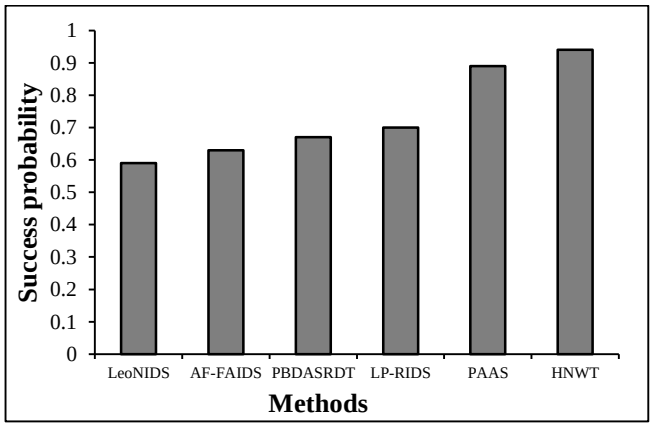

Fig.16. Flooding attack probability comparison

In Fig.16, comparison evaluation of the success probability for the proposed and existing methodologies is given. From this comparison it can be proved that proposed method HNWT tends to have better performance than previous methodologies with accurate detection of attacker nodes. From this comparison it is proved that proposed HNWT shows 5.61% higher attack

detection probability than PAAS, 34.28% higher attack detection probability than LP-RIDS, 40.29% higher attack detection probability than PBDASRDT, 49.2% higher attack detection probability than AF-FAIDS and 59.32% higher attack detection probability than LEoNIDS.

5. CONCLUSION

In this research work, Hybrid Node Watching Technique (HNWT) is introduced for the accurate DDoS flooding attack detection. This research technique attempt to find the variation in the data's and control messages transmitted between the end nodes to find the flooding attack presence. This is done through the trust nodes which are selected optimally by using cat swarm algorithm. These optimally selected nodes will monitor data transmission behaviour to predict malicious node presence. The overall implementation of this research work is done in NS2 simulation environment from which it is proved that proposed research technique tends to have increased attack detection rate.

REFERENCES

[1] E. Fadel, V.C. Gungor, L. Nassef, N. Akkari, M.A. Malik, S. Almasri and I.F. Akyildiz, "A Survey on Wireless Sensor Networks for Smart Grid", *Computer Communications*, Vol. 71, pp. 22-33, 2015.

[2] B. Rashid and M.H. Rehmani, "Applications of Wireless Sensor Networks for Urban Areas: A Survey", *Journal of Network and Computer Applications*, Vol. 60, pp. 192-219, 2016.

[3] K. Chelli, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", *Proceedings of World Congress on Engineering*, pp. 23-29, 2015.

[4] D. Pridhi and R. Gargi, "Energy Need Minimization by Power Aware Routing In WSN", *International Journal of Recent Research Aspects*, Vol. 3, No. 2, pp. 41-45, 2016.

[5] K. Kaushal and V. Sahni, "Early Detection of DDOS Attack in WSN", *International Journal of Computer Applications*, Vol. 134, No. 13, pp. 1-14, 2016.

[6] T. Kaur, K.K. Saluja and A.K. Sharma, "DDOS Attack in WSN: A Survey", Proceedings of International Conference on Recent Advances and Innovations in Engineering, pp. 1-5, 2016.

[7] S. Deore, and A. Patil, "Survey Denial of Service Classification and Attack with Protect Mechanism for TCP SYN Flooding Attacks", *International Research Journal of Engineering and Technology*, Vol. 3, No. 5, pp. 1-14, 2016.

[8] G. Singh and P. Gupta, "To Alleviate the Flooding Attack and Intensify Efficiency in MANET", *Proceedings of International Conference on Secure Cyber Computing and Communication*, pp. 87-94, 2018.

[9] A. Hassanzadeh, R. Stoleru and J. Chen, "Efficient Flooding in Wireless Sensor Networks Secured with Neighborhood Keys", *Proceedings of International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 119-126, 2011.

[10] A.H. Moon, U. Iqbal, G.M. Bhat and Z. Iqbal, "Simulation and Analysing RREQ Flooding Attack in Wireless Sensor Networks", *Proceedings of International Conference on Electrical, Electronics, and Optimization Techniques*, pp. 3374-3377, 2016.

[11] S. Bhalodiya and K. Vaghela, "Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol", *International Journal of Computer Applications*, Vol. 125, No. 4, pp. 1-17, 2015.

[12] A.R. Prusty, "The Network and Security Analysis for Wireless Sensor Network: A Survey", *International Journal of Computer Science and Information Technologies*, Vol. 3, No. 3, pp. 1-14, 2012.

[13] P. Rolla and M. Kaur, "Dynamic Forwarding Window Technique against DoS Attack in WSN", *Proceedings of International Conference on Micro Electronics and Telecommunication Engineering*, pp. 1-7, 2016.

[14] Y. Ping, H. Yafei, Z. Yiping, Z. Shiyong and D. Zhoulin, "Flooding Attack and Defence in Ad Hoc Networks", *Journal of Systems Engineering and Electronics*, Vol. 17, No. 2, pp. 1-13, 2006.

[15] N.S. Chouhan and S. Yadav, "Flooding Attacks Prevention in MANET", *International Journal of Computer Technology and Electronics Engineering*, Vol. 1, No. 3, pp. 1-12, 2011.

[16] S.K. Shandilya and S. Sahu, "A Trust based Security Scheme for RREQ Flooding Attack in MANET", *International Journal of Computer Applications*, Vol. 5, No. 12, pp. 1-11, 2010.