DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5328

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

DISTRIBUTED AGENT BASED TECHNIQUE FOR DETECTING DISTRIBUTED DENIAL-OF-SERVICE (DDoS) ATTACKS IN WLAN

Er. Harmeet Singh
Research Scholar
Department of Computer Science & Engineering, SBBS University, Jalandhar, India

Dr.Vijay Dhir
Professor
Department of Computer Science & Engineering, SBBS University, Jalandhar, India

Abstract: By sending large amount of data flows from multiple sites, Distributed Denial-of-Service (DDoS) attacks target the victims. Thus, there is a demand to implement number of DDoS defense techniques all together and collaboratively on many nodes, especially on where there is a need to maintain round-the-clock Internet connectivity. The security mechanism works on a probabilistic basis that is based on the detection of illegitimate traffic and then to discard it, that forced a specific number of legitimate packets to be fallout in the process and reducing the overall quality of service. In this paper a Distributed Agent Based technique for detecting DDoS Attacks in wireless LAN has been proposed. It is fully distributed and provides an early warning when pre-attack activities are detected, using trust mechanisms. From the simulation results it has been found that the proposed distributed agent based architecture achieves high throughput with low packet drop, by detecting and isolating the attack traffic flows.

Keywords: DDoS, WLAN,

1. INTRODUCTION

1.1 THREATS TO WIRELESS LAN

Wireless Local Area Networks (WLANs) have many possible disturbing threats. The security issues which affect the WLAN are the various attacks including Denial of Service (DoS) and mis-configured wireless access point (WAP). In addition to the number of attacks on wired networks, a there are few specific attacks vulnerabilities in the wide array of 802.11 affect the wireless networks. For protecting and detecting these possible threats, an intrusion detection and prevention system must be used by the wireless networks. Intrusion detection system solution is also important for the organizations which do not have a WLAN due to the dangerous wireless threats [1, 18, 22, 24, 25, 26].

A misbehaving Wireless Access Point (WAP) is introduced into the wireless networks 802.11which attacks and collects the sensitive data from the WLAN. Even the users introduce the misbehaving nodes. WLANs can be improved well on combining the advantages of the less expense and trouble-free installation along with the mobility. A backdoor can be created into the network by implementing a WAP on an identified WLAN [1, 18].

Many location-based wireless defense techniques & routing protocols are affected by the wormhole attack. The existing wireless network routing protocols are not able to find the routes lengthy than two or more hops if there is no mechanism for defending wormhole attacks which disrupts communication severely. [11, 15, 19].

Wormhole helps in the networking services as it offers a lengthy network link to the link layer and up which is useful for the attacker to use that link. The flow of data is disrupted by modifying data packets, creating unwanted routing activities, selectively dropping and turning off the wormhole link periodically, when the attackers utilize a high volume of network traffic during the wormhole. [14, 17, 20].

In this paper an attempt has been made to propose a fully distributed approach for early warning, when pre-attack activities are detected, using trust mechanisms.

The remaining paper is organized in the different sections. Section II discuss the research work done in the field. Section III presents the Distributed Agent Based detection Technique for DDoS. Section IV presents the results and discussion. In last Section -V conclusions are presented.

1.2 PREVIOUS WORK

In the last few years a large number of studies have been done by various researchers.

In the previous work, a MAC layer based defense architecture for the Reduction of Quality (RoQ) attacks in Wireless LAN was designed for the detection and prevention of intruders in WLAN [1].

In the second work, a cross-layer based intrusion detection technique for wireless local area networks was designed. In this technique a combined weight value was computed from the RSS and TT. If the weight value is greater than a threshold value, then the corresponding node is considered as an attacker. Significant results were obtained using proposed techniques [2].

As continuation in the previous works, detection technique for the wormhole attacks are proposed in this paper.

1.3 DDOS (DISTRIBUTED DENIAL OF SERVICE) ATTACKS

DDoS attacks commonly overthrow the channel by sending enormous packets from various attack sites. As a result the channel wastes its important resources. During extensive attacks, DDoS traffic also generates a intense congestion in the Internet which disturbs the normal communication between all Internet users [1].

There is only one approach to fully eradicate the DDoS attack is by securing the various nodes on the Internet

© 2015-19, IJARCS All Rights Reserved

against misuse that is impractical. Generally major spots currently handle the issues with critical approaches. This will creates the barrier for the attacker.

The prevention and detection of DDoS is remain open challenges and there is need to develop defenses approach for the detection of attacks and responsive system by falling excess traffic.

DDoS attacks are triggers by the victim, source and the intermediate networks means the three major components of network. From the destination, it is very easy to detect an attack at the destination as compared to the source because destination generate high volume of traffic that source [2].

There is need to implement number of approaches simultaneously and collaboratively on the wireless networks to protect various nodes from the attackers. There are number of approaches introduces by adding digital signatures and encryption features, but these are relative complex, more overhead, and more delay to the network,. The prevention and detection mechanism is need to address for providing the quality of services.

In this paper an Intelligent Agent Based Defense (IABD) Architecture for DDos Attacks was proposed, which is fully distributed and provides an early warning when pre-attack activities are detected, using trust mechanisms.

Znaidi et al. [4] have proposed a mechanism for securing, defending and detecting wormhole attack in wireless networks. This mechanism considering local and neighborhood information and not necessitating the other parameters such as location information, clock synchronization or dedicated hardware. Furthermore, the algorithm is also not dependent on the wireless communication models. The limitation of this mechanism is that, a wormhole link could be detected only if the actual distance between the any two wormhole nodes is greater than four-hop because of the computed coefficients.

Xu et al. [5] have proposed a distributed wormhole detection algorithm (DWDA) in the basis of network disorder detection initiated by the presence of a wormhole. In this algorithm a hop-counting approach was used as an investigation procedure for the wormhole attack detection and then rebuilds local maps in all node. Later, it uses a "diameter" feature to detect irregularities triggered by wormholes. The key benefit of using DWDA approach is that it can provide the approximate location of a wormhole that helps the researcher for designing further defense approaches.

Win et al. [6] had addressed the various wormhole attack detection methods for wireless networks. In this paper they addressed approach exercised in the DaW security model which combines a defense and detection approach for wormhole attack by using false positive, false negative and precision of alarm performance parameters. The alarms were compared with LF analysis and found to be more specific. The performance of the approach was measured using ns-2 simulations and found that the proposed routing protocol was performed much better in terms to attain low delay.

Hu et al. [7] have presented a challenging attack to defend against a wormhole attack in a wireless networks, and propose a new method for defending and detecting wormhole. In this approach a packet leashes method was proposed to detect wormhole attacks using following types of leashes (i) geographic leashes and (ii) temporal leashes. Finally, an efficient authentication protocol was designed, called TIK by using temporal leashes.

Ronghui et al. [8] have introduced a simple and effective approach locate and detect wormhole attack. This approach was based on the idea of location discovery in wireless networks using hop counting method. This algorithm also provides an estimation of location of wormhole in wireless networks.

Kaissi et al. [9] have presented a new protocol called DAWWSEN having a defence and detection approach against the wormhole attack, a powerful attack that has serious consequences on sensor routing protocols. The main advantage of this algorithm is that it works without the time stamp of the packet for detecting a wormhole attack and does not need any geographical information about the nodes. This is an imperative parameter for the resource confined behavior of the sensor nodes. In future work, some modifications can be introduced to our routing protocol in order to get a balanced tree where the load would be fairly distributed among the nodes since this will considerably help in reducing the value of Trefresh.

Choi et al. [10] developed a secure and effective mechanism without using special support of hardware called Wormhole Attack Prevention (WAP). The mechanism provide detection as well as prevention in wireless networks. They proposed an effective mechanism based on dynamic source routing protocol. The major benefit of this approach is that it can work without time synchronization of the location information. Their future work is to study false negative and false positive rate problems for the detection of wormholes.

Phuong et al [12] have presented a transmission time based approach for the detection of wormhole attacks in wireless networks. The proposed approach is used for the detection of wormhole by computing the transmission time (TT) between established path of two successive nodes. Attack is identified by transmission time between two fake nodes created by wormhole and this transmission time is significantly higher between the two real nodes that are within the range.

Sriram et al. [13] have proposed a classification for the various possible wormhole attack using an infrastructure based wireless networks. They had proposed a detection approach by using Neighbor Discovery and Link Verification parameters. These parameters are used to observe traffic in and out of its adjoining access point and uses of first-hop and second-hop neighbors' data structure. This approach decrease the risk of wormhole attacks and does not need any location information and clock synchronization.

Recently, many researchers have proposed intrusion detection techniques for wireless sensor networks [3,16, 21-24].

© 2015-19, IJARCS All Rights Reserved

2. AGENT BASED DEFENSE ARCHITECTURE

2.1 SYSTEM ARCHITECTURE AND OVERVIEW

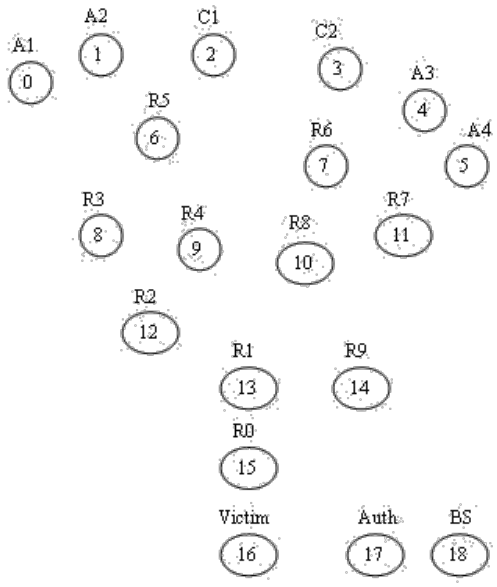

Figure 1: System Architecture

In our proposed architecture, many autonomous agents tend to protect the internal system network. In any possible attack related scenarios, the agents will sent alert messages for the network administrator. Each agent will execute a security monitoring function at a specified node and monitor the network traffic data against any attacks. Figure 1 presents the sample network topology with four attackers (marked as A1, A2, A3 and A4) and two legitimate clients (marked as C1 and C2). The bottom most node (marked as victim) is the victim node. It also consists of one BS (node 18). The attack related alert messages are send to this BS by the agents. There is an authenticator placed between the victim and the BS in order to verify the alert messages.

Each agent monitors the traffic in a cost effective manner at a *superflow* level. This level comprises all packets destined from all possible source IP for the same network domain and having the same prefix IP address of the same destination domain. It also operates different protocols such as UDP or TCP etc that detects the cumulative from individual flows.

The detection approach is proposed at the agent level for the detection of sudden variations in the flows of traffic. When a DDoS attack is triggered, the agents which are deployed initially, monitor variation in spatiotemporal distribution of volumes of traffic. Typically, these variations in traffic flows are towards the direction of the victim node, whereas random fluctuations occurred due to legitimate traffic flows will not be in the direction of the victim. Based on these changes, these agents exchange traffic surge reports with each other, and collaboratively detect the attacker. Then an alert message is send upstream towards the source node.

The DDoS attacks are detected by using an agents, initially deployed near the source. Then the process is continued from agent to agent, dynamically towards the victim.

2.2 AGENT BASED DDOS DETECTION

Each agent monitors change in traffic and computes the amount of received packets in a particular time window at each I/O port. All packets of a super flow must be directed towards the same destination network.

Let t1, t2,…, tn be the time intervals.

FOR INCOMING TRAFFIC:

Let NP_{tk} be the amount of received packets by an agent Ai at time tk.

We can define the historical approximation of average number of packets as:

$$AVGNP_{tk} = (1 - \lambda) . AVGNP_{t(k-1)} + \lambda . NP_{tk} \quad (1)$$

Where $0<\lambda<1$ is sensitivity factor showing the long-term average performance to the current traffic change.

Then the change of the input traffic dvi_{tk} from the average by time k is given by

$$dvi_{tk} = dvi_{tk-1} + NP_{tk} - AVGNP_{tk} \quad (2)$$

In DDoS attack, the total deviation is significantly more than the random fluctuations. Since the deviation of input traffic is sensitive to the traffic changes, we calculate the abnormal deviation of input traffic *AVGdv* from historical average as:

$$AVGdv_{tk} = dvi_{tk} / AVGNP_{tk} \quad (3)$$

If $AVGdv > \delta$, where δ is the detection threshold that represents attack traffic. The value of δ can be fixed based on the previous detection results.

If $AVGdv < \delta$, then there is no DDoS attack.

FOR OUTGOING TRAFFIC

Let NP_{tk} be number of packets leaving at time k.

Then the deviation of the output traffic dvo_{tk} from the average at time k is given by

$$dvo_{tk} = dvo_{tk-1} + NP_{tk} - AVGNP_{tk} \quad (5)$$

Where $AVGNP_{tk}$ is the historical average leaving packets determined similar to (1).

If $AVGdv > \delta$, then calculate $dvio_{tk}$,which is defined as the ratio of incoming and outgoing traffic deviations, which is calculated using (2) and (5) as,

$$dvio_{tk} = dvo_{tk} / dvi_{tk} \quad (6)$$

Through monitoring the *dvio* value, an agent decides whether deviation is due a DDoS attack.

If *dvio* is close to 1 (one), the traffic aggregation pattern is considered suspicious. The agent then triggers an alert message and also intimate the pattern to the source. Otherwise the agent will sends a repeated message regarding status, indicating that there is no any anomaly observed.

3. TRUST AMONG AGENTS

In our distributed agent based IDS, we are using the concept of trust mechanism among the agents. In our agent based system, each agent depends on the reports of other agents. As intruders will try to attack any node in the network, agents has to check the trust of other agents, to identify the

© 2015-19, IJARCS All Rights Reserved

compromised agent nodes. If any agent finds that the received report from any other agent does not match with the expected results, it can be considered as a compromised agent node.

Each agent i maintains a trust index T for all the other agents, which is updated for each report it receives from the other agents.

(i) If the agent i, receives a report from the agent k , then , trust index of k is calculated as

$$Tik = (MRk - NRk) / n \quad (1)$$

Where MRk is the number of reports that matches with agent i's report. NRk is the number of reports that does not match with agent i's report. n is the number of messages received in the time period tn.

(ii) If agent k's report is different from agent i's report, then agent i checks Tik. If Tik <

Tth, where Tth is the trust threshold, then agent i broadcast a trust request message TReq to other agents. TReq contains the node id suspected agent node.

(iii) On receiving TReq, the agents send their corresponding trust index value of agent k, as a trust reply message TRep.

(iv) After collecting the trust reply messages TRep from other agents, the agent i once again checks If Tjk < Tth , where Tjk is the trust index value of agent k, collected from agents j, j=1,2… (j <> k) . If the condition is true for atleast m agents (m < j) , then the agent k is considered as compromised . Any report from that agent will be discarded.

4. SIMULATION RESULTS

In this section, the performance of the proposed algorithm has been evaluated. In order to test the proposed protocol, the NS2 simulator [15] is used. The proposed Distributed detection techniques has been compared with the normal wormhole attack scenario without applying any detection techniques.

4.1 PERFORMANCE METRICS

For evaluating the performance of the proposed technique following metrics have been used:

- Attack Bandwidth – Attack bandwidth is the amount of bandwidth affected by the attackers (in Mb/s)
- Attack Packets Drop – Attack Packets Drop is the number of packets of the attackers that are detected and eliminated by the monitoring agents.

In this experiment, the performance of proposed distributed agent based technique has been evaluated.

A. BASED ON RATE

In the first experiment the traffic rate was varied as 200Kb to 500Kb.

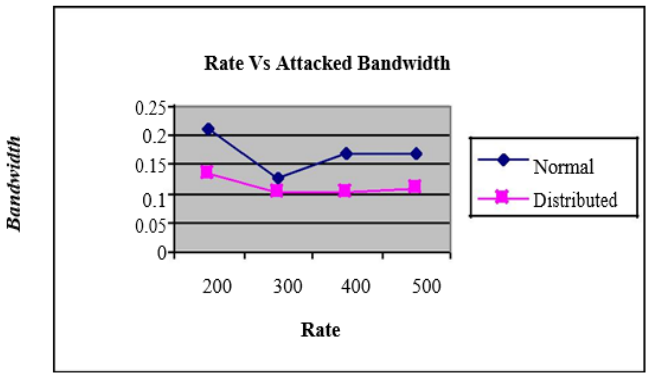

Fig 2: Rate Vs Bandwidth

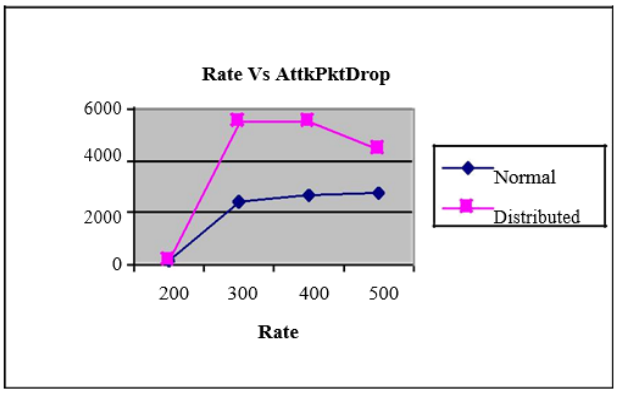

Fig 3: Rate Vs Packets Dropped

Figure 2 shows the bandwidth affected or occupied by the attackers when the attack traffic rate is increased. From the figure it is clearly seen that in the distributed scenario, the amount of attack bandwidth is less when compared to the normal scenario, which indicates that the adverse effect of attackers is reduced in the distributed case.

From Figure 3, it is clearly shown that the number of attack packets dropped when the traffic rate is increased. From the results it has been found that the distributed approach eliminates most of the attack packets when compared to the normal approach.

B. BASED ON TIME

In the second experiment, the simulation time interval was varied from 5 to 25 seconds.

© 2015-19, IJARCS All Rights Reserved

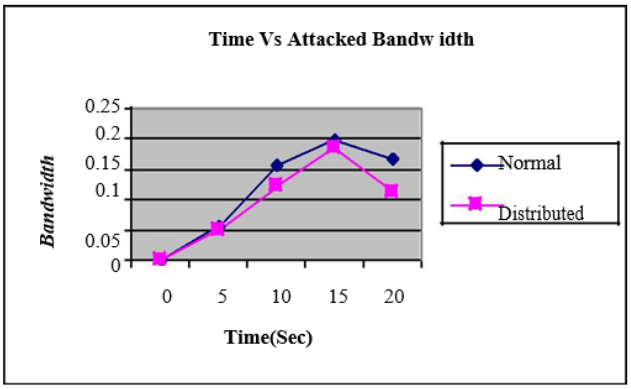

Fig 4: Time Vs Attacked Bandwidth

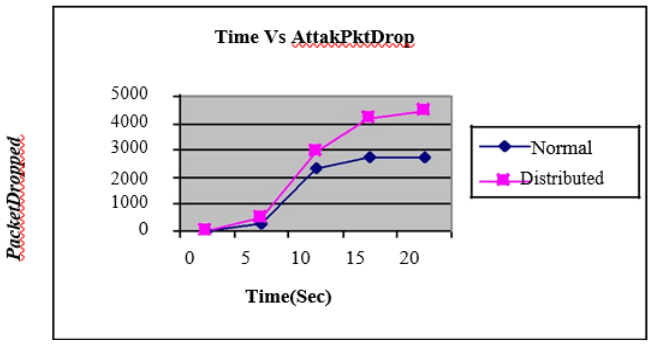

Fig 5: Time Vs Attack Packets Dropped

Figure 4 shows that the bandwidth affected or occupied by the attackers when the time interval is increased. From the graph it is clearly visible that in the distributed scenario, the amount of attack bandwidth is less when compared to the normal scenario, which indicates that the adverse effect of attackers is reduced in the distributed case. From Figure 5 it is clearly shown that the number of attack packets dropped when time interval is increased from 0 to 20 seconds. From the experimental results it has been analyzed that the distributed approach eliminates most of the attack packets when compared to the normal approach.

5. CONCLUSION

In this paper, a Distributed agent Based technique for detecting DDoS Attacks in wireless LAN has been proposed. The main advantage of the proposed technique is that it provides an early warning when pre-attack activities are detected. The agents proposed in the architecture are autonomous, mobile and cooperative entities. Each agent executes a detection algorithm and based on the detection results, it exchanges its report with other agents. Based on the collaborative report, a final alert is sent to the base station. Further a trust mechanism in which each agent checks the trust of other agents, to identify the compromised agent nodes has been designed. If any agent finds that the received report from any other agent does not match with the expected results, it can be considered as a compromised agent node. Through simulations, it has been proved that the proposed architecture achieves high throughput with low packet drop, by detecting and isolating the attack traffic flows. Therefore the proposed technique can be used for the detection of DDoS attacks in wireless LAN.

REFERENCES

[1]. J. Singh, S. Gupta and L. Kaur, “A MAC Layer Based Defense Architecture for Reduction of Quality (RoQ) Attacks in Wireless LAN”, International Journal of Computer Science and Information Security, Vol. 7, Issue 1, pp. 284-291, 2010.

[2]. J. Singh, S. Gupta and L. Kaur, “Taxonomy of Attacks in Wireless Local Area Networks”, Journal of Research in Computer Engineeri ng, Vol.4, No. 1, 2010.

[3]. J. Mirkovic, M. Robinson, P. Reiher and G. Oikonomou, “Distributed defense against DDoS attacks” University of Delaware, CIS Department Technical Report CIS-TR-2005-02, pp. 1-12, 2005.

[4]. A. Challita, M.E. Hassan, S. Maalouf, A. Zouheiry, “A Survey of DDoS Defense Mechanisms”, Department of Electrical and Computer Engineering, American University of Beirut, 2004.

[5]. M. Robinson, J. Mirkovic, M. Schnaider, S. Michel and P. Reiher. "Challenges and principles of DDoS defense." In ACM SIGCOMM. 2003.

[6]. W. Znaidi, M. Minier and J.P. Babau, “Detecting wormhole attacks in wireless networks using local neighborhood information." In proceedings of IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1-5, 2008.

[7]. Y. Xu, G. Chen, J. Ford and F. Makedon, “Distributed wormhole attack detection in wireless sensor networks." In Proceedings of the First Annual IFIP Working Group International Conference on Critical Infrastructure Protection, 2007.

[8]. K.S. Win, “Analysis of detecting wormhole attack in wireless networks", In World Academy of Science, Engineering and Technology, pp. 422-428, 2008.

[9]. Y. C. Hu, Y. Chun, A. Perrig and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks." In IEEE Twenty-Second Annual Joint Conference of the Computer and Communications, Vol. 3, pp. 1976-1986, 2003.

[10]. H. Ronghui, M. Guoqing, W. Chunlei and F. Lan, “Detecting and locating wormhole attacks in wireless sensor networks using beacon nodes”, World Academy of Science, Engineering and Technology, Vol. 3, 2009.

[11]. R.Z. El Kaissi, A. Kayssi, A. Chehab and Z. Dawy, “DAWWSEN: A defense mechanism against wormhole attacks in wireless sensor networks”, Ph.D. Dissertation, American University of Beirut, Department of Electrical and Computer Engineering, 2005.

[12]. S. Choi, D.Y.Kim, D.Y. Lee and J. Jung, "WAP: Wormhole attack prevention algorithm in mobile adhoc networks." In IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pp. 343-348, 2008.

[13]. T.V. Phuong, N.T. Canh, Y.K. Lee, S. Lee and H. Lee, “Transmission time-based mechanism to detect wormhole attacks”, In 2nd IEEE Asia-Pacific Service Computing Conference, pp. 172-178, 2007.

[14]. V.S.S. Sriram, A.P. Singh and G. Sahoo, "Methodology for Securing Wireless LANs against Wormhole Attack”, International Journal of Recent Trends in Engineering, Vol. 1, no. 1, 2009.

[15]. Network Simulator, http://www.isi.edu/nsnam/ns

[16]. M. Shojaei, N. Movahhedinia and B.T. Ladani, "DDoS attack detection in IEEE 802.16 based networks”, Wireless Networks, Vol. 20, Issue 8, pp. 2543-2559, 2014.

[17]. M. GhasemiGol, A. Ghaemi-Bafghi, M. Moghaddam and H. Sadoghi-Yazdi, “Anomaly detection and foresight response strategy for wireless sensor networks”, Wireless Networks, Vol. 21, Issue 5, pp. 1425-1442, 2014.

[18]. T.V.P. Sundararajan, S. M. Ramesh, R. Maheswar and K.

© 2015-19, IJARCS All Rights Reserved

R. Deepak, "Biologically inspired artificial intrusion detection system for detecting wormhole attack in MANET", Wireless Networks, Vol. 20, Issue 4, pp. 563-578, 2014

[19]. G. Koutepas, F. Stamatelopoulos and B. Maglaris, "Distributed management architecture for cooperative detection and reaction to DDoS attacks", Journal of Network and Systems Management, Vol. 12, Issue 1, pp. 73-94, 2004.

[20]. T. Thapngam, S.Yu, W. Zhou and S.K. Makki, "Distributed Denial of Service (DDoS) detection by traffic pattern analysis" Peer-to-Peer Networking and Applications, Vol. 7, Issue 4, pp. 346-358, 2014.

[21]. G. Lee, W. Kim, K. Kim, S. Oh and D. Kim, "An approach to mitigate DoS attack based on routing misbehavior in wireless ad hoc networks", Peer-to-Peer Networking and Applications, Vol. 8, Issue 4, pp. 684-693, 2013.

[22]. K. Verma, H. Hasbullah and A. Kumar, "Prevention of DoS attacks in VANET", Wireless Personal Communications, Vol. 73, Issue 1, pp. 95-126, 2013.

[23]. G. Chen, Y. Zhang and C. Wang, "A wireless multi-step attack pattern recognition method for WLAN", Expert Systems with Applications, Vol. 41, Issue 16, pp. 7068-7076, 2014.

[24]. M. Andreolini, M. Colajanni and M. Marchetti, "A collaborative framework for intrusion detection in mobile networks", Information Sciences, Vol. 321, pp. 179-192, 2015.

[25]. J. Singh and R.Singh "WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks", Mobile Information Systems, Vol.6, 2016.

[26]. V.Dhir, R.Kumar and V.Joshi "Performance comparison of routing protocols in mobile ad hoc networks" International Journal of Engineering Science and Technology,Vol.2, pp. 3494-3502, 2010.

© 2015-19, IJARCS All Rights Reserved