DOI: http://dx.doi.org/10.26483/ijarcs.v9i3.6038

ISSN No. 0976-5697

Volume 9, No. 3, May-June 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

HYBRID TRACE BACK TECHNIQUE FOR PREVENTING DDOS ATTACK ON WIRELESS SENSER NETWORKS

Manoj Pathak
Computer Science& Engineering,
Adina Institute of Science& Technolog,
RGPV, Sagar, India

Rajneesh Pachouri
Computer Science& Engineering,
Adina Institute of Science& Technolog,
RGPV, Sagar, India

Anurag Jain
Computer Science& Engineering,
Adina Institute of Science& Technolog,
RGPV, Sagar, India

***Abstract*—** Wireless sensor network (WSN) is combinations of large number of nodes which are of limited capabilities, to collect sensitive information's. Security is main problem in such type of wireless sensor networks. There are a few system assaults conceivable on WSN and distributed denial of service (DDos) assault is one of them. They focus on a wide assortment of essential assets, from banks to news sites, and present a noteworthy test to ensuring individuals can distribute and get to imperative data. There are lots of methodologies implemented to detect and prevent the DDos attack on wireless sensor network but they all suffer from some weakness. To overcome these weaknesses we have proposed a hybrid traceback method (combination of ip logging and packet marking method) for prevention of DDos attack on wireless sensor network.

Keywords— WSN, DDoS, packet marking, ip logging

I. INTRODUCTION

Late advances in remote correspondences and modernized contraptions have enabled the headway of straightforwardness, low-control, multifunctional sensor center points that are little in measure and pass on untethered in short partitions. These minor sensor hubs, which comprise of detecting, information handling, and imparting parts, use the possibility of sensor systems in light of community oriented exertion of countless. Remote Sensor Networks have been generally connected in different fields, for example, ecological observing, social insurance administration, war zone reconnaissance and industry control. Wireless sensor network (WSN) associates the appropriated self-sufficient sensors for gathering the information from sensors or disseminate the information into sensors. They impart over a short separation and work together to achieve any assignment. The point of security system in WSN is to monitor the data from assaults. This security instrument which is accommodated Wireless sensor network ensures that system administrations are accessible in nearness of any weakness. There are security system depends on five standards [1] confidentiality, authentication, Integrity, accessibility and information freshness.

The Denial of Service (DoS) assault much of the time sends undesirable bundles and it tries to use the data transmission of system. It legitimates the system client from getting to the framework or assets when required. The DoS assault can introduce itself in physical layer, connect layer, organize layer and transport layer. DoS assault can be counteracted by solid validation and distinguishing proof incorporated with the interruption location framework. Different DoS assaults are extremely cruel and it responds in two courses, for example, sticking and altering. Sticking is the consider impedance on the remote correspondence channel. This assault is a basic one in which the assailant tries to disturb the tasks of whole system or a specific little bit of it. Sticking might be reliable or sporadic. To deal with sticking at organize layer manages mapping sticking region in the system or in neighbouring steering zone. The assault is straightforward and compelling when the system is based on single recurrence generally the assault ought to be disposed of since it utilizes different types of spread range. Altering is one of the physical assaults, which focuses on the equipment of the sensor hubs. Altering assault isn't practical to oversee several hubs reach out finished a region of a few kilometers. Altering aggressors may uncover the delicate data like cryptographic key from hub by harming it to get access to more elevated amount of correspondence. The main security instrument against hardening is to temper-proof physical bundling. Be that as it may, it costs extra.

II. RELATED WORK

Shi-Jinn Horng et al [2] have outlined another stream for interruption location framework utilizing SVM strategy. The famous KDD Cup 1999 dataset was utilized to assess the proposed framework. Contrasted and other interruption identification frameworks that depend on the same dataset, this framework indicated better execution in the discovery of DoS and Probe assaults, and the best execution in overallaccuracy.

Hayoung Oh et al [3] have proposed a constant interruption and irregularity discovery framework utilizing SOM. This framework marks the guide created by SOM

utilizing relationships between's highlights. It orders neurons as ordinary or assaults. On account of assault neurons, they have grouped them again into the kinds of assaults. At the point when a noxious conduct is gotten, this framework recognizes the interruption as beforehand known assault or another untrained assault.

Mohammad Wazid [4] has utilized hybrid anomaly detection technique procedure with the k-means clustering. WSN are mimicked utilizing OPNET simulator and the resultant dataset comprises of movement information with end to end defer information which has been grouped utilizing WEKA 3.6. In this examination, it has been watched that two kinds of abnormalities (confusion and dark opening assaults) are initiated in the system.

Shun-Sheng Wang et al [5] have planned an integrated intrusion detection system using intrusion dataset from UCI vault .The dataset prepared well utilizing BPN and the yield is utilized as an essential parameter in ART model to group the information. At long last the yields got from the two methods are thought about and the ART display gives the best exactness rate and general execution.

Mohit Malik et al [6] have connected the rule based method for identifying the security assault in WSN. They have found ten essential security assault compose in their work and the parameters of those assault have been created fluffy administer based framework for figuring the effect of security assault on the remote sensor arrange. Once the framework has been executed it demonstrates the effect of assault in the system.

Reda M. Elbasiony et al [7] have proposed a hybrid detection framework i.e. in anomaly detection, kmeans clustering algorithm is utilized to identify novel interruptions by bunching the system association's information to gather the greater part of interruptions together in at least one bunches. In this proposed cross breed system, the oddity part are enhanced by supplanting the k-implies calculation with another called weighted k-implies calculation, In this methodologies Knowledge Discovery and Data Mining (KDD'99) datasets are utilized.

LeventKoc et al [8] have proposed another method HNB demonstrate which shows a prevalent general execution regarding precision, blunder rate and misclassification cost .In beginning periods the customary Naïve Bayes display are utilized yet the outcome delivered by HNB is superior to conventional Naïve Bayes. The outcomes they have delivered demonstrate that this model altogether enhances the exactness of recognizing denial-of-services (DoS) assaults.

WenyingFenga et al [9] have presented another method for consolidating calculation for the better outcome in distinguishing interruptions. They have grouped the system exercises into typical or strange by lessening the misclassification rate. In this work the creator consolidated Support Vector Machine technique and the Clustering in light of Self-Organized Ant Colony Network to take the focal points by maintaining a strategic distance from their shortcomings. This Experiments show that CSVAC (Combining Support Vectors with Ant Colony) defeats better the SVM or CSOACN to the extent both portrayal rate and run-time capability.

MeghaBandgaret al [10] have portrayed a novelapproach utilizing Hidden Markov Models (HMM) to identify Internet assaults and they have depicted around an interruption recognition framework for distinguishing a mark based assault. They have performed single and different HMM show for source partition both on IP and port data of source and goal. In this approach they have diminished the false positive rate.

Dat Tran et al [11] have proposed Fuzzy Gaussian blend demonstrating strategy for organize oddity location. In this work a blend of Gaussian circulations are utilized to speak to the system information in multi-dimensional component space. Utilizing fluffy C-implies estimation, Gaussian parameters were assessed and the entire work is done with the KDD Cup informational collection. The proposed strategy created here is more successful than the vector quantization technique.

VahidGolmah [12] has been created a cross breed strategy utilizing C5.0 and SVM calculation and they have researched and assess the execution of this half breed method with DARPA dataset. The inspiration for utilizing this half and half approach is to enhance the exactness of the interruption recognition framework when contrasted with utilizing individual SVM and C50. By consolidating the SVM and C5.0 this strategy took less of execution time.

Punam Mulak [13] has utilized cross breed procedure by consolidating Boundary cutting calculation and grouping calculation. The inspiration for utilizing this half and half approach is to enhance the precision of the interruption location framework and to give preferable outcome over other grouping.

Venkata Suneetha Takkellapati [14] has proposed another framework where Information Gain (IG) and Triangle Area based KNN calculation are utilized for choosing more discriminative highlights. At that point Greedy k-implies bunching calculation is joined with SVM classifier to recognize Network assaults. This framework accomplishes with high exactness location rate and less mistake rate .All this work are completed in KDD CUP 1999 preparing informational collection.

Vaishali Kosamkar [15] has taken after same strategy of joining C4.5 Decision Tree and Support Vector Machine (SVM) calculation keeping in mind the end goal to accomplish high precision and lessen the false alert rate. In highlight determination arrange, Correlation-Based Feature Selection (CFS) calculation is utilized for better precision result.

HarmeetKaurl [16] has composed their work to decrease the deferral in the system and to deliver end to end information in great speed. So keeping in mind the end goal to accomplish, they have reenacted WSN utilizing SPEED convention. They have utilized two execution parameters throughput and vitality utilization for investigation. BCO (Bee Colony Optimization) calculation is utilized to give better outcomes with high throughput and low vitality utilization. Every one of the recreations are completed in MATLAB.

III. METHODOLOGY

The defence architecture for DDOS attack will be used to detect Attackers. Defence Framework provides following important features:

1. To make a TTL(time to live) and framework table and store it on the switches.
2. To coordinating of a TTL esteem with any passage of the table is characteristic of the way this is the primary switch on the way.
3. The switch should then check the bundle with its IP address.

4. Select the variable length alternatives field in the IP header for checking reason.
5. To over compose the IP packet with the genuine IP address of the switch if the attacker forges the choices field with wrong IP address or pointless information.
6. To tackle satirizing by a system called Ingress Filtering in which the switch disposes of the bundles with ill-conceived source addresses.
7. To check the authenticity of source address can be checked from the system id part of the IP address.
8. For more powerful answer for IP Traceback is to join Ingress Filtering with this variation of parcel stamping (in view of TTL distinguishing proof).
9. To actualize the Algorithm in Network Simulator (NS-2) condition.
10. for Implementing the Algorithm first, we will write TCL files in the NS-2
11. Then we will use our technique to Mark the IP packets using DPM.
12. In next step the TTL is check for each incoming packet using NS-2
13. Finally we will analyze the total no of packet drops in the System.

PROPOSED WORK

We propose a new IP traceback technique which is a variant of packet marking and is based on TTL identification. This technique was initially proposed for IPv4 networks.

Figure 1: Flow Chart for the proposed IP traceback technique

Different IP traceback techniques have been proposed so far. Some of them are compatible with existing infrastructure and some require modification to it, but the effectiveness of any traceback technique can be measured by the following characteristics.

1. Capability of tracing any type of DoS attack.
2. Minimum overhead in terms of storage requirements.
3. Minimum processing requirements on the routers.
4. Least complexity in path reconstruction algorithm (if any).
5. Faster convergence.

This hybrid technique was proposed by taking into account all the above mentioned characteristics. The aim of all the traceback techniques is to identify the sources of attacking traffic but path reconstruction algorithms actually reveal the identity of first router on the path. A superior approach is discover an algorithm that uncovers the character of first router without requiring the support of the considerable number of routers on the way. Since the attacker can produce any field in the IP header, he can't distort the Time to live (TTL) field. The TTL is a 8-bit field that decides the most extreme number of bounces a datagram can cross. Each switch decrements the TTL regard by 1, in the wake of sending the datagram.The issue of deciding the primary switch on the way can be tackled by utilizing this field. The TTL field is diverse for various working frameworks and isn't generally chosen, however every one of the parcels sent by a specific working framework will have a similar starting TTL esteem. We propose to make a TTL versus working framework (OS) table and store it on the switches. The switch should read the TTL estimation of the considerable number of bundles going through it. If the TTL value matches any entry of the table, the router should mark the packet with its identification. This router would obviously be of the subnet from which the packets originated. All the other routers on the path cannot mark the packet, since the TTL value would not match any entry of the TTL vs. OS table. There is one exception to this. Consider a packet originating with a TTL of 64. It would be marked by its subnet router. But after four hops, its TTL would be 60. Since 60 is an entry of stored table, the packet would again be marked. On the off chance that this packet was sent by an attacker, traceback would prompt a subnet four bounces from the subnet from which the assault began. To defeat this issue, we propose to utilize the reserved flag in IP header (there are 3 flags in IP header, 2 are utilized with fragmentation and one is saved). The main switch on the way should set the flag to '1' in the wake of denoting the bundle. The various switches on the way should read both the TTL and reserved flag. The packet should only be marked if a match of TTL is found and the value of reserved flag is ‘0’. It is however not possible that a packet originating with a TTL of 255 would reach a router with its TTL set to 128 since 95% of the traffic in the internet reaches its destination before 30 hops. The storage requirements on the routers can be minimized by having only a 5 entry TTL table.

The proposed marking scenario obviously has the first two characteristics of an effective IP traceback technique. We can trace any type of DoS attack because each and every packet is marked by its subnet router. It is possible to trace DoS attacks which require only a single packet, which may not be possible with other marking techniques like PPM and iTrace.

The second challenge is obviously to store the marking information. The question arises where to store the marking information in the IP header. Basic DPM uses the 16-bit ‘Identification’ field of the IP header. However, choosing Identification field may not be a good idea because it is used for fragmentation purposes. Fragmented traffic constitutes between 0.25% and 0.5% of the total IP traffic. In spite of the fact that the measure of divided activity is little, it does exist and for the most dire outcome imaginable, Identification field ought to be saved just for fragmentation purposes. Conveying checking data in outbound packets (iTrace) would clearly expand router and system overhead and would require another and complex convention to be actualized also. We propose to utilize the Record Route (RR) discretionary field in the IPv4 header. The IP address of the router would be stored in the first 4 bytes of route data in RR field. Thus, the router appends the marking information with the packets. If the RR field is already present, the router should overwrite the first 4 bytes of route data in it. Thus, even if the attacker forges the RR field with wrong IP addresses or unnecessary data, it would still be overwritten with the true IP address of the router. The minimum required length of RR field is 7 bytes (4 bytes for route data, 1 byte for option type code, 1 byte for option length and 1 byte for pointer into the route data). The remaining space in the optional field can be used for other options like ‘Strict Source Route’, ‘Loose Source Route’, ‘Stream Identifier’ etc, if required.

IV. RESULTS AND DISCUSSION

What Every trackback approach attempt is to precisely distinguish the wellsprings of assaulting activity yet way re-development calculations in systems really uncover character of first switch on the way. More suited approach is discover a

calculation that can discover the character of first switch without requiring the commitment of the considerable number of switches in the way. As the trespasser can fashion any field in the IP header, he can't manufacture.

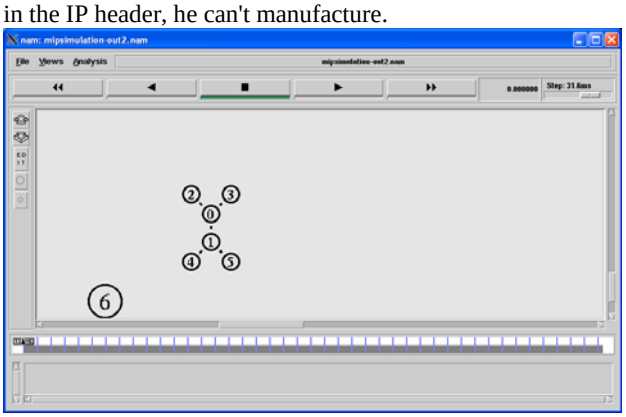

Figure 2: Simulated Topology in Network Simulator for Traceback

Node 6 has more bandwidth than all combined The TTL is an 8-bit field that determines the maximum number of hops a datagram can traverse. Every switch decrements the TTL esteem by 1, in the wake of sending the datagram. The issue of deciding the primary switch on the way can undoubtedly be tackled by using this field.

The span of the topology doesn't make a difference since all the postponement is caused at the main switch as it were. Movement started from hub 7 and was bound for hub 3. For this movement, hub 0 goes about as the principal switch on the way. Activity comprised of TCP bundles of 1040 bytes conveying FTP information.

The extra time taken by checked activity is only 0.8 milliseconds. Similar delay is also observed for traffic from node 13 to node 8 for which node 12 acts as the first router on the path.

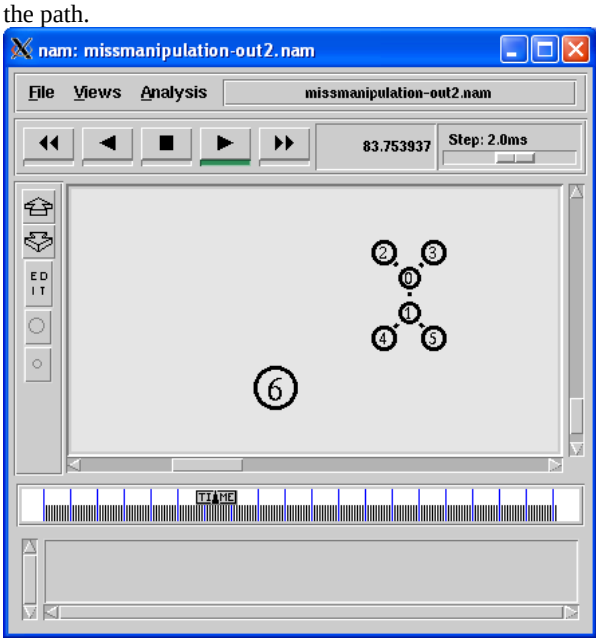

Figure 3: initialization of Network Traffic

In fig 3 the simulated topology starts the initialization of Network Traffic, initially most of the traffic comes from legitimated sources.

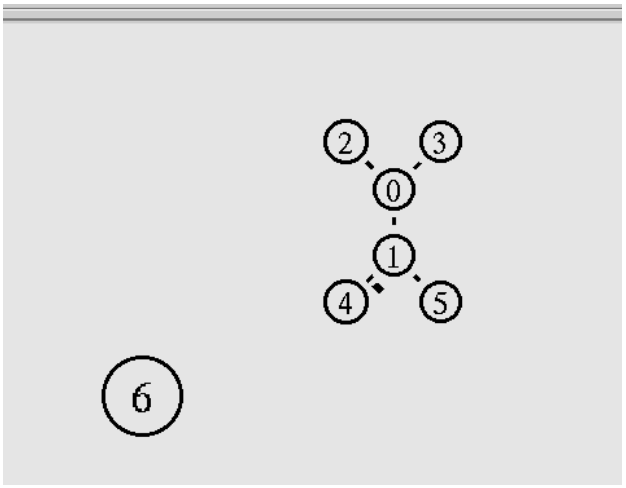

Figure 4: ACK of received packets is being done in normal fashion.

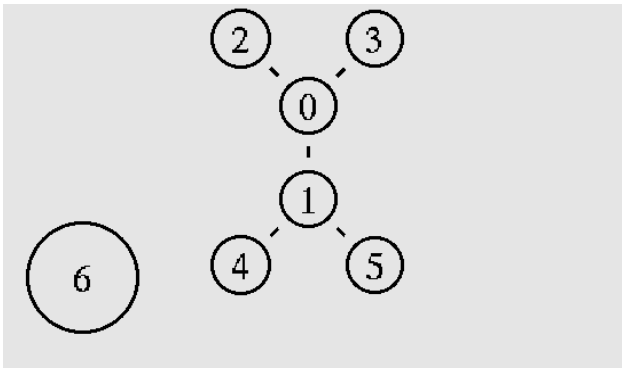

Figure 5: Attacker Draws near the Network.

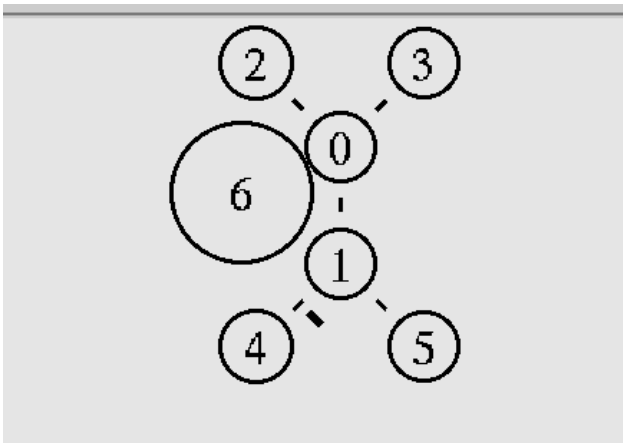

Figure 6: Using TTL field to trace Source packets of the incoming traffic.

Time to live handle Time to live (TTL) or jump restrain is a system that constrains the life expectancy or lifetime of information in a PC or system. TTL might be executed as a counter or timestamp joined to or installed in the information.

Once the prescribed event count or time span has elapsed, data is discarded. In computer networking, TTL prevents a data packet from circulating indefinitely.

The network was in the normal mode in beginning. The packet delay and header overhead for traffic was traced into suitable output. Then the TTL field was modified and recompiled. Afterwards, Simulating the same network topology.

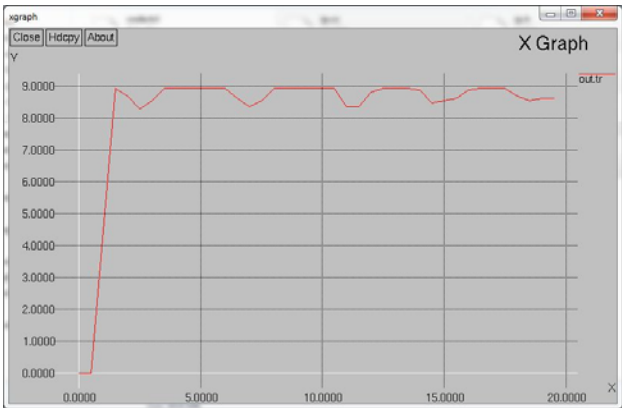

Figure 7: Overhead Caused by Zombies in the Network.

The overhead and delay was found as network is looking to readjust. This traffic overhead depends on the type of underlying application or service utilized for sending data. The graph in figure 7 shows delay caused by DDoS traffic.

This section describes the parameters used in the simulations. The performance simulation environment used is based on NS-2, a network simulator that provides support for simulating multi-hop wireless networks complete with physical and IEEE 802.11 MAC layer models.

In this section, we analyze the effect of different prevention techniques and shows that our proposed technique is better than existing prevention technique. Table 5.3 and Figure 5.9 show the effect of proposed prevention technique on Throughput with different number of attackers. This figure shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent. Table 2 and Figure 7 demonstrate the impact of proposed aversion procedure on Number of Collisions with various number of aggressors and it likewise indicates examination with the current counteractive action conspire. This figure demonstrates that proposed avoidance method (By crippling IP Broadcast) relieve the impact of flooding based DDoS assault with bigger degree. By utilizing this procedure number of impacts diminishes when contrasted with the crashes of existing avoidance plot.

Table 1: Effect of Proposed Prevention Technique on Throughput with varying number of attackers.

Attacker	Throughput
1	1714653
2	1617242
3	1530967

Table 2: Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers.

Attacker	Existing	Proposed
1	3955	2655
2	4018	2595
3	4175	2676
4	4210	1818
5	4315	2084

V. Conclusion and Future Scope

Taking care of DDoS attacks in WSNs is rapidly ending up increasingly mind boggling, and has achieved the point where it is hard to see zombies spread all through system. On one hand, this thwarts a comprehension of the DDoS marvel. The assortment of known assaults makes the feeling that the issue space is huge, and difficult to investigate and address. For grouping assaults and resistances analysts needs a superior comprehension of the issue and the present arrangement space. The attack characterization criteria in WSNS is significantly more troublesome. Subsequent to investigating existing structures, we have discovered three kinds of DDOS systems: casualty end resistance structures, source-end protection structures, and appropriated guard structures. It is past the point of no return for casualty end resistance systems to react to DDOS attacks. A source-end barrier structure can't accomplish great execution because of absence of assault data. Interestingly, an appropriated structure can accomplish better execution by collaborating among disseminated numerous safeguard subsystems. We propose traceback approachs to control undesirable activity by moderating flooding based DDOS assaults. The work focuses chiefly on the recognition calculation ought to recognize a DDOS assault at the starting source with high unwavering quality. Two principle necessities for skilled traceback are to quickly and accurately discover conceivable aggressors and other is to channel assault bundles with the goal that a host can continue the ordinary capacity to genuine customers. The greater part of the proceeding with IP traceback techniques center around seeking after the district of assailant's after the assault. This work, we actualized a proficient procedure for finding conceivable aggressors who hold the DDOS-based attacks.

References

[1] Kumar Singh 1, M P Singh 2, and D K Singh, "ASurvey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks", International Journal of Computer Trends and Technology- May to June Issue 2011.

[2] Horng, Shi-Jinn, et al. "A novel intrusion detection system based on hierarchical clustering and support vector machines." Expert systems with Applications 38.1 (2011): 306-313.

[3] Hayoung Oh," Attack Classification based on Data Mining Technique and its application for Reliable Medical Sensor Communication", International Journal of Computer Science and Applications, Vol.6, No. 3, pp 20 – 32, 2009.

[4] Mohammad Wazid , " Hybrid Anomaly Detection using K-Means Clustering in Wireless Sensor Networks" ,Center for Security, Theory and Algorithmic Research, pp. 1-17.

[5] Shun-Sheng Wang, Kuo-Qin Yan , Shu-Ching Wang , Chia-Wei Liu ,"An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks", Elsevier, pp. 15234–15243, 2011.

[6] Mohit Malik, Namarta kapoor, Esh naryan, Aman Preet Singh," Rule Based Technique detecting Security attack for

Wireless Sensor network using fuzzy logic", International Journal of Advanced Research in Computer Engineering & Technology,Volume 1, Issue 4, , ISSN: 2278 – 1323, June 2012.

[7] Reda M. Elbasiony , Elsayed A. Sallam , Tarek E. Eltobely ,Mahmoud M. Fahmy ," A hybrid network intrusion detection framework based on random forests and weighted k-means" Ain Shams Engineering Journal", vol 4, pp.753–762,2013.

[8] Levent Koc , Thomas A. Mazzuchi, Shahram Sarkani,"A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier", Elsevier,pp.13492–13500, 2012.

[9] Wenying Fenga, Qinglei Zhangc, Gongzhu Hud, Jimmy Xiangji Huange, "Mining network data for intrusion detection through combining SVMs with ant colony networks", Elsevier , pp. 127-140, 2013

[10] Megha Bandgar, Komal dhurve, Sneha Jadhav,Vicky Kayastha,Prof. T.J Parvat, " Intrusion Detection System using Hidden Markov Model (HMM)", IOSR Journal of Computer Engineering (IOSRJCE)

e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 3, pp.66-70, (Mar. - Apr.2013).

[11] Dat Tran, Wanli Ma, and Dharmendra Sharma,"Network Anomaly Detection using Fuzzy Gaussian Mixture Models", International Journal of Future Generation Communication and Networking, pp.37-

42, 2012.

[12] Vahid Golmah, " An Efficient Hybrid Intrusion Detection System based on C5.0 and SVM", International Journal of Database Theory and Application Vol.7, No.2 ,pp.59-70, (2014).

[13] Punam Mulak, Nitin R. Talhar, "Novel Intrusion Detection System Using Hybrid Approach", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 11, ISSN: 2277 128X, November 2014.

[14] Venkata Suneetha Takkellapati1 , G.V.S.N.R.V Prasad," Network Intrusion Detection system based on Feature Selection and Triangle area Support Vector Machine", International Journal of Engineering Trends and Technology-Volume3Issue4- 2012

[15] Vaishali Kosamkar, Sangita S Chaudhari,"Improved Intrusion Detection System using C4.5Decision Tree and Support Vector Machine",International Journal of Computer Science and Information Technologies, Vol. 5 (2) , pp. 1463-1467, 2014

[16] Levent Koc , Thomas A. Mazzuchi, Shahram Sarkani,"A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier", Elsevier,pp.13492–13500, 2012.

.

