



slaves and is controlled by the master hacker. IRC(Internet Relay Chart) a command & control server is used by attacker to provide instruction to bots. In this paper we discuss how DDoS attack the wireless sensor network & the techniques to avoid the DDoS attack.

## 2. Literature Review

Marco Tiloca et. al. proposed industrial applications and factory automation for Wireless Sensor Networks[8]. The authors have worked closer to TDMA based WSNs. They have proposed an algorithm named SAD-SJ for the protection against DDoS attack on networks. Md. Monzur Morshed et. Al. proposed Cluster Based Secure Routing Protocol (CBSRP) is a MANET routing protocol with ensurity of secure key management and secure communication taking place between mobile nodes[9].They have used digital signature and hashing technique to facilitate the secure communications. Seuwow. P. et. al. have proposed Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs) [10]. They have worked upon vanet security to protect against various attacks. Qian.yi et.al. have worked on the performance evaluation of a secure MAC Protocol for vehicular network[11].They have proposed a quality of service (call priority) based MAC protocol to enhance the security ofthe VANETs. Javed.M.A. et. al. have developed a Geocasting technique in an IEEE802.11p based vehicular Ad hoc network for road traffic management[12]. A location aware packet transmission based technique is used to protect against various VANET security issues. Hung c.c.et.al. proposed Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks[13]. According to this paper traditional ad hoc routing protocols are not well suited for these high dynamic network. In this paper they propose a new Heterogeneous Vehicular Network (HVN) architecture and a mobility pattern aware routing for HVN.Dias .A.J. et.al. have created a Test bed environment based Performance Evaluation of Routing Protocols for VehicularDelay-Tolerant Networks[14].

## 3. Proposed Model

The aim of this research project is to develop an effective and new method to protect against the selective jamming attacks (a form of distributed denial of service attack). A new technique is developed based on the unique code exchange in the inter-transmission topology packets to ensure the integrity of the neighbour nodes. The random unique code is sent to the neighbour nodes for the integrity insurance purposes. The integrity insurance is a technique to prevent the unauthorized nodes from communicating with the nodes in the wireless sensor network. In the base paper, the SAD-SJ technique has been used to protect against the selective jamming denial of service attacks, which has performed well in the case of denial of service attack. Denial of service attack is a form of network availability attacks. When a single node tries to compromise the availability of the network, it is called a denial of service attack. In the existing technique, authors have used a statically dynamic codes embedded in the packets. These codes are used to detect the integrity of the neighbour nodes. In case, an attacker tries to attack the

WSN, the packets sent from attacker node is blocked by the WSN nodes when they detect the absence of unique code embedded in the inter-transmission packets.

We have analyzed the existing security mechanism thoroughly. We have found that the random code generation technique used in the existing paper can be generated using an algorithm and can be regenerated and used to forge the wireless network nodes and take the authorization by establishing communication link with the WSN nodes to launch the selective jamming attack. To mitigate the threat of regeneration of the secure code, we have used the time to live field as the security code. The time to live security field can't be forged in the IP packet header, whereas all of the other fields can be easily forged using header structure manipulation scripts. TTL codes are generally different for different operating systems. WSN nodes usually works on the embedded Linux or other simple and light embedded operating systems based on Linux. The default TTL codes for various wireless sensor node operating systems are applicable in the case of proposed algorithm. The basic idea behind our proposed model is to create a TTL table for every operating system being used for wireless sensor nodes and stored on all of the wireless sensor nodes. The network node initially requests its sensor nodes to send their TTL code and a local neighbour table based on TTL codes is formed. The TTL code is matched on each node with the code sent from the neighbour node initially, when a packet is received on it. In the case, any abnormality is found in a stream of packets, the communication with the abnormal node is blocked. For the inter-transmission topology packet marking, the variable length TTL field in the IP header is used.

The selective jamming DDoS attack uses IP flooding to make the network resources unavailable. The problem of this packet flooding is solved by a technique called Ingress Filtering. Ingress filtering is a technique, in which the wireless sensor node discards the packets with illegitimate source addresses by scanning and matching the TTL field. The legitimacy of neighbour node is checked from the time to live field in the of the IP header by matching with the neighbour table based on unique codes formed on the initial stage.

**Table 1:** Default initial TTL values for Different Operating Systems

OS	Version	Platform	TTL
Digital Unix	4.0	Alpha	60
Unisys	X	Mainframe	64
Linux	2.2.x	Intel	64
FTX (UNIX)	3.3	STRATUS	64
Cisco	11.2	7507	60
Cisco	12.0	2514	255
IRIX	6.x	SGI	60
Free BSD	3.x	Intel	64
Open BSD	2.x	Intel	64
Solaris	8	Intel / Sparc	64

Advantages of new algorithm:

- Reduced marking overhead due to ingress filtering.
- No need of address reconstruction.
- Faster convergence.
- Usability of identification field is retained for fragmentation purposes.
- Reliable approach to identify the ingress router.

#### Algorithm 1: Secure Code Marking Algorithm Flow

1. Wireless sensor node Nx in a cluster taken initial stage startup
2. Nx sends own information to the neighbour nodes
3. Neighbour nodes Ny-Nz respond with their information
4. Nx sends own secure code information to neighbour node
5. Ny-Nz respond with their secure transmission to Nx
6. Nx builds and populates a secure code based neighbour table
7. All Nodes start inter-communication after building neighbour relationship and populating neighbour table
8. Nx receives packets from Ny
9. Nx examines the secure code in packets with the neighbour table build at initial neighbour relationship formation stage
10. If secure code matches, Nx authorize Ny and accept the ingress packet stream
11. If secure code does not match, Nx block Ny and reject the ingress packet stream
12. Nx receives packets from Ny-Nz
13. Nx examines the secure code in packets with the neighbour table build at initial neighbour relationship formation stage
14. If secure code matches, Nx authorize Ny-Nz and accept the ingress packet stream
15. If secure code does not match, Nx block Ny-Nz and reject the ingress packet stream
16. Denial of service attack mitigated on step 11 & 15

## 4. Result Analysis

The proposed algorithm has been implemented in NS-2 installed on ubuntu Linux platform on system equipped with Inter-i3 CPU/2 GB RAM/1 GB GPU/500 GB HDD. The proposed model is based on the Layer 3 of ISO model to facilitate the IP network communication between the network nodes. Internet Protocol (IP) has been modified to for incorporating marking using TTL field for the secure communication using authentication and authorization to differentiate between the actual neighbour node and attackers launching distributed denial of service attack. The IP protocol in the ns-2 simulation model was modified using a TCL script and some of the editing has been made to the simulator programming files written in C++ to incorporate secure code marking in it. The running model is based on the resulting scenario implemented after the recompilation and activation of the changes made to the source code. The topology size is kept limited to avoid the confusion and overload of the packet transmissions visualizations. The modified internet protocol is thoroughly

tested on all of the nodes to minimize the effect of the DDoS attack on the WSN cluster. The changes have been observed in amount of delay and overhead when implemented then secure code framework in the simulation.

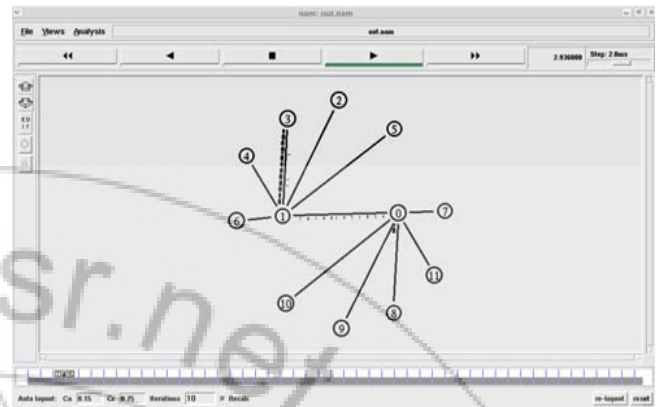


Figure 1: The Simulation Topology

The function of all other nodes except the traffic ingress procedure remains the same. The normal scenario simulated in NS-2 is shown in the snapshot displayed in Figure 1.



Figure 2: Graph showing delay for the marked and normal traffic.

The delay and overhead has been recorded to analyze the performance of the proposed model where the IP protocol has been modified to facilitate the secure code marking to detect the false/attacker nodes in the wireless sensor network. The network simulation after the incorporating the proposed model for secure code marking/embedding has resulted in the minimized overhead & delay as shown in the simulation results in figure 2. The overhead is based on the traffic/application/service type used in the simulation, like, CBR and VBR. It also depends upon the packet size offered by the service/application/traffic used in the simulation. The graph in figure 2 shows delay and overhead comparison of the normal and secure marked traffic. This shows the efficiency of this technique.

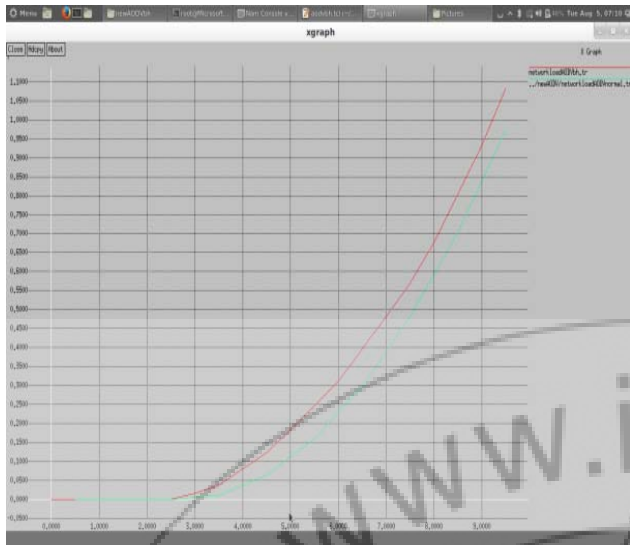


Figure 3: Network Load Comparison Graph

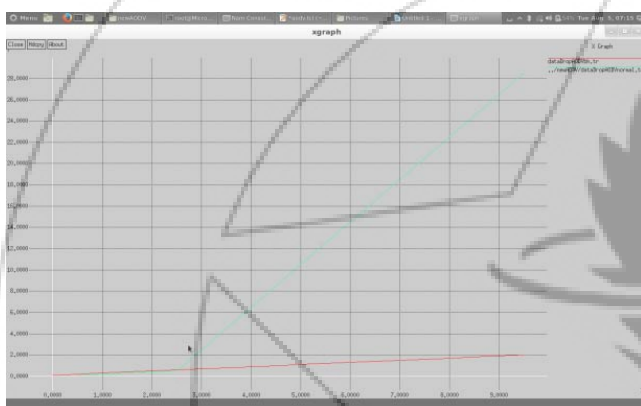


Figure 4: Data Drop Normal Comparison Graph

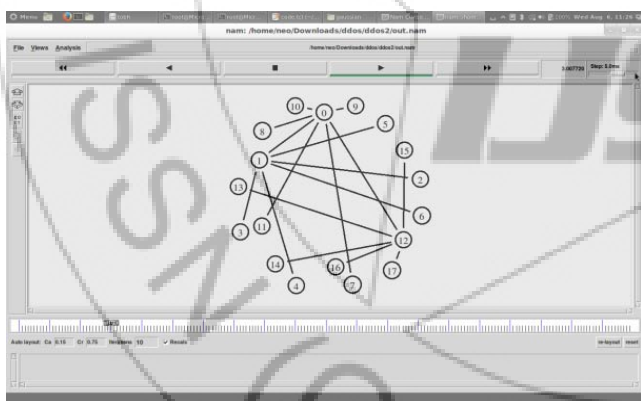


Figure 5: Network Topology

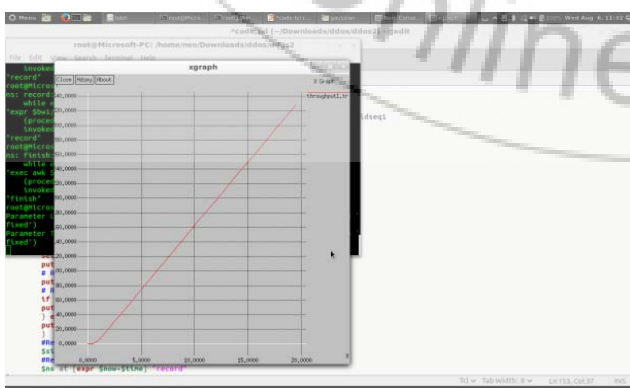


Figure 6: Network Load in the normal network Cluster

It has been observed from the results that the throughput and network load is higher under the simulation scenario implemented with proposed scheme rather than the existing scheme. The network load is the parameter of total load in the network. The total load is measured by the calculating total computational power used in the network cluster. The data drop and network load is comparatively higher in the normal network cluster, whereas in the cluster with the proposed solution has shown the significant improvement in the network performance

### 5. Conclusion

The development of the secure code marking technique is the result of the analysis of the various DDoS attacks in the recent years. There are many existing traceback techniques to mitigate DoS and DDoS attacks. Almost all was to study & analyze the existing DoS or DDoS mitigation and to design the fool proof solution to mitigate DDoS attacks on WSNs. The effectiveness of any DDoS attack mitigation technique depends basically on the computational overhead, network convergence and the effectiveness of the technique to detect the DDoS attacks. However, the source node traceback using secure code marking or any other technique is the first step in identifying the attacker node correctly. The proposed hybrid DDoS attack mitigation technique is capable of tracing the selective jamming DDoS attack or any other form of DDoS attacks. Because the node is capable of tracing every single packet, it enhances the effectiveness of the DDoS mitigation technique. In this research, the gap of the WSN DDoS attack mitigation has been filled using the effective and strong secure code marking based DDoS mitigation technique which makes all WSN nodes individually capable of mitigating DDoS attack on their own.

### References

- [1] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 8, pp. 2-23, year 2006.
- [2] Yun Zhou, Yuguang Fang, Yanchao Zhan, Securing Wireless Sensor Networks: A Survey, IEEE Communications Surveys & Tutorials, year 2008.
- [3] Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page 53-57, year 2004.
- [4] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006.
- [5] Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009.
- [6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks, IEEE Communications Magazine, 40(8):102-114, August 2002.

- [7] Healy.M, Newe.T, Lewis.E, „Security for Wireless Sensor Networks: A Review“, IEEE Sensor Application Symposium, New Orleans, LA, USA-Feb 17-19, 2009.
- [8] Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi, “SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks”, ETFA, vol. 18,pp. 1-8, IEEE, 2013.
- [9] Md. Monzur Morshed, Md. Rafiqul Islam,“CBSRP: Cluster Based Secure Routing Protocol”, IACC, vol. 3, pp. 571-576, IEEE, 2013.
- [10] Patrice Seuwou, Dilip Patel, Dave Protheroe, George Ubakanma“Effective Security as an ill defined Problem in Vehicular Ad hoc Networks (VANETs)”.
- [11] Yi Qian ,Kejie Lu , and Nader Moayeri“PERFORMANCE EVALUATION OF A SECURE MAC PROTOCOL FOR VEHICULAR NETWORKS” (2008 IEEE)
- [12] Muhammad A. Javed and Jamil Y. Khan “A Geocasting Technique in an IEEE802.11p based Vehicular Ad hoc Network for Road Traffic Management”. (2010).
- [13] Chia-Chen Hung, Hope Chan, and Eric Hsiao-Kuang Wu “Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks”( IEEE WCNC 2008).
- [14] João A. Dias, João N. Isento, Vasco N. G. J. Soares, Farid Farahmand, and Joel J. P. C. Rodrigues “Testbed-based Performance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks” (2011 IEEE).