# Secure Data Transmission with Hybrid Cryptographic Technique in Wireless Sensor Networks

**Pradeepa.B[1] Anand.C[2] Gnanamurthy.R.K[3]**
[1]Student of M.E [2]Assistant Professor [3]Principal
[1,2,3]Department of Computer Science & Engineering
[1,2]KSR College of Engineering, Anna University, Namakkal, Tamilnadu 637215, India [3]SKP Engineering College, Anna University, Thiruvannamalai, Tamilnadu 606611 , India

*Abstract*— Denial of service (DoS) attack cause severe crash on computing system. To shield our system from dos attack is a crucial task. In the existing system, Multivariate Correlation Analysis (MCA) procedure is used to sense the attacks by anomaly detection method. This gives contribution capable of detecting recognized and unidentified dos attacks successfully by knowledge the prototype of genuine network traffic only. But this method cannot recognize some unfamiliar dos attack. To conquer this dilemma, the proposed method employs two cryptographic system which gives security to both the data and users. Polynomial bi-variate key endow with security to the users by detecting the authorized users to admittance the data in the network. One way hash chain algorithm endow with security to the data. In this system, hash data and wrapped key is an additional security added by every intermediate node. In conclusion the destination user decrypt all the hash data and keys gets the unique message. These methods will exactly sense the attackers.

***Key words:*** Denial-of-service (DoS) attack, polynomial bi-variate key, one way hash chain

## I. INTRODUCTION

The Denial of Service attacks in the wireless sensor networks are the notable attacks that need to be contained. There exists a certain limit of data to be transmitted through a medium between the legitimate users. This transfer of data is unaffected if the flow is within the competence level of the medium. But in case of intrusion of a compromised user or an attacker (zombies), they try to flood the normal traffic with unlimited packets of data into the medium. The flooding of data packets causes the medium to be congested leading to the denial of service to the intended users.

A simple network can be constructed using the same protocols and such that the Internet uses without actually connecting it to anything else. A specialized field in computer networking that involves securing a computer network infrastructure. Network security is typically handled by a network administrator or system administrator who implements network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access and also ensure that employees have adequate access to the network and resources to work. A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network.

Wireless Sensor Networks (WSNs) can be utilized for a wide range of applications and services that often require high level security. This security encompasses a large number of challenges ranging from the nature of wireless communications, deployment model of the network, unattended environment, large and dense network, disconnected network, presence of physical stimuli, etc. Examples of some of the security-sensitive applications of WSN are; moving object tracking, intruder detection in a particular area, patient monitoring in hospital while the patient data are to be kept secret, military reconnaissance, volcano monitoring, disaster management and warning system, and the like. In addition to ensuring confidentiality and fidelity of acquired data, these applications demand smooth transmission of information throughout the network. This requires unscathed service and continuous availability of network resources for the full duration of the network's operation. However, the sensors that build up a WSN are generally low-cost devices that are equipped with limited memory, processing, radio, and battery reserves. Moreover, considering the conditions of low-cost deployment of WSN and tiny size of sensors, it is difficult to increase the capabilities of sensors even with the state-of-the-art technology. In wireless sensor network, the goal is to ensure the best possible utilization of sensor resources so that the network could be kept functional as long as possible. In contrast to this crucial objective of sensor network management, a Denial of Service (DoS) attack targets to jeopardize the efficient use of network resources and disrupts the essential services in the network. Because of the wide range of methods used for creating a denial of service situation in the network, DoS attack could be considered as one of the major threats against WSN security.

In this proposed system, to protect our information from attackers is essential task. For that we use cryptographic technique that will protect our system from attackers. Polynomial bi-variate key provides security to user and one way hash chain gives security to data.

Polynomial bi-variate key provides security to the user by detecting authorized users to access the information in the network. One way hash chain technique gives security to the data that are passing from source to destination. Hash data and wrapped key are added with data at every intermediate node. These two techniques provides more security to the users and data from attackers.

## II. RELATED WORKS

**W.Zhou et al [2]** used a Distributed Denial of Service (DDoS) attack is a critical threat to the Internet, and botnets are usually the engines behind them. Sophisticated botmasters attempt to disable detectors by mimicking the traffic patterns of flash crowds. This poses a critical challenge to those who defend against DDoS attacks. In our deep study of the size and organization of current botnets,

 

we found that the current attack flows are usually more similar to each other compared to the flows of flash crowds. Based on this a discrimination algorithm using the flow correlation coefficient as a similarity metric among suspicious flows. They formulated the problem, and presented theoretical proofs for the feasibility of the proposed discrimination method in theory. Our extensive experiments confirmed the theoretical analysis and demonstrated the effectiveness of it.

**G. Thatte et al [3]** used parametric methods to detect network anomalies using only aggregate traffic statistics, in contrast to other works requiring flow separation, even when the anomaly is a small fraction of the total traffic. By adopting simple statistical models for anomalous and background traffic in the time domain, one can estimate model parameters in real time, thus obviating the need for a long training phase or manual parameter tuning. The bi-variate parametric detection mechanism (bPDM) uses a sequential probability ratio test, allowing for control over the false positive rate while examining the tradeoff between detection time and the strength of an anomaly.

**Y. Chen et al [4]** used to develop a distributed change-point detection (DCD) architecture using change aggregation trees (CAT). The idea is to detect abrupt traffic changes across multiple network domains at the earliest time. Early detection of DDoS attacks minimizes the flooding damages to the victim systems serviced by the provider developed a system that is built over attack-transit routers, which work together cooperatively. Each ISP domain has a CAT server to aggregate the flooding alerts reported by the routers. CAT domain servers collaborate among themselves to make the final decision. To resolve policy conflicts at different ISP domains, a new secure infrastructure protocol (SIP) is developed to establish mutual trust or consensus.

**M. Tav et al [5]** used KDD'99 is built based on the data captured in DARPA'98 which has been criticized by McHugh, mainly because of the characteristics of the synthetic data. As a result, some of the existing problems in DARPA'98 remain in KDD'99. However, there are some deliberate or unintentional improvements, along with additional problems. In the following we first review the issues in DARPA'98 and then discuss the possible existence of those problems in KDD'99. Finally, we discuss new issues observed in the KDD data set.

## III. CRYPTOGRAPHIC TECHNIQUE

In the proposed system, data is transmits from the source to destination through several nodes, where each node called a intermediate node and which having a verification key. When that key is correct then only node can read the data after that it will send to next node. Likewise the data is passing through several nodes finally reach the destination. By using cryptographic method, we are giving the protection to the data which are transmitting from source to destination. Not only data gets secured from the attacker we also giving protection to the user who are transmit and receiving the data.

Polynomial bi-variate key is used to provide the security to the users. Polynomial bi-variate key is generated for all the sensor node in the network .by using this key, only authorized user can transmit and receive the data in the network also generating the random number for nodes to identify user. One way hash key algorithm is used to provide the security for records or data. When the packets are transmit from each node, a hash data is added with the packets by user and send to the receiver. Finally the receiver decrypts all the hash data and gets the original data.

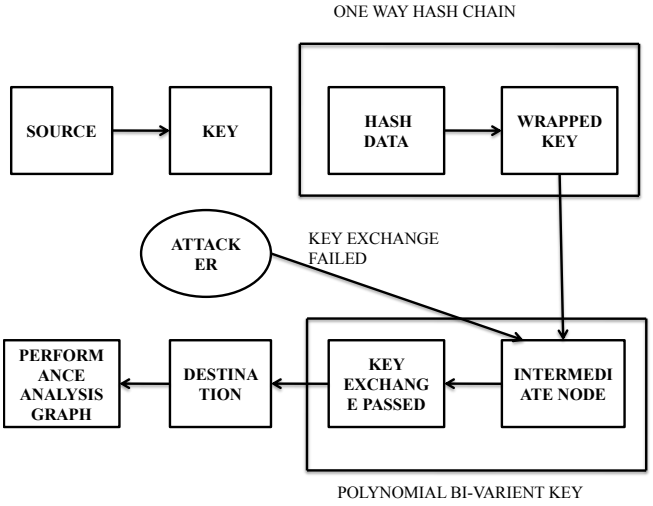


Fig. 1: Architecture diagram

## IV. KEY EXCHANGE MECHANISM

This module used to generate the polynomial bi-variate keys for all sensor nodes in wireless sensor network. The purpose of polynomial bi-variate key is to identify the user is authorized or not. Using this polynomial bi-variate key, only authorized person can transmit and receive data's in the network. Polynomial key is to provide the security for user.

### *A. Polynomial Bi-variate Key:*

The bi-variate polynomial is generated by using the following equation. The polynomials have the property of

- P(a,b)=P(b,a).
- P (a,b) = $^{i}b^{j}$ ,
- c (ij) =c (ji)
- Where,
- c (ij) denotes communication cost
- a ,b denote the node ID

The identification number is added with each polynomial to differentiate the polynomials. For each node in the network, we preload the subset of n polynomials from polynomial pool. For each polynomial share preloaded in a node m is P (a, b).

## V. HYBRID CRYPTOGRAPHIC TECHNIQUE

In this module is used for generate the hash data by using one way hash chain algorithm. One-way chains are an important cryptographic primitive in many security applications. As one-way chains are very efficient to verify, they recently became increasingly popular for designing security protocols for resource-constrained mobile devices and sensor networks, as their low-powered processors can compute a one-way function within milliseconds, but would require tens of seconds or up to minutes to generate or verify a traditional digital signature

 

### *A. One Way Hash Chain Technique:*

One-way chains are an important cryptographic primitive in many security applications. As one-way chains are very efficient to verify, they recently became increasingly popular for designing security protocols for resource-constrained mobile devices and sensor networks, as their low-powered processors can compute a one-way function within milliseconds, but would require tens of seconds or up to minutes to generate or verify a traditional digital signature. Recent sensor network security protocols thus extensively use one-way chains to design protocols that scale down to resource-constrained sensors.

A one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input. Here "easy" and "hard" are to be understood in the sense of computational complexity theory, specifically the theory of polynomial time problems. Not being one-to-one is not considered sufficient of a function for it to be called one-way hash chain is the successive application of a cryptography hic hash function to a piece of data.

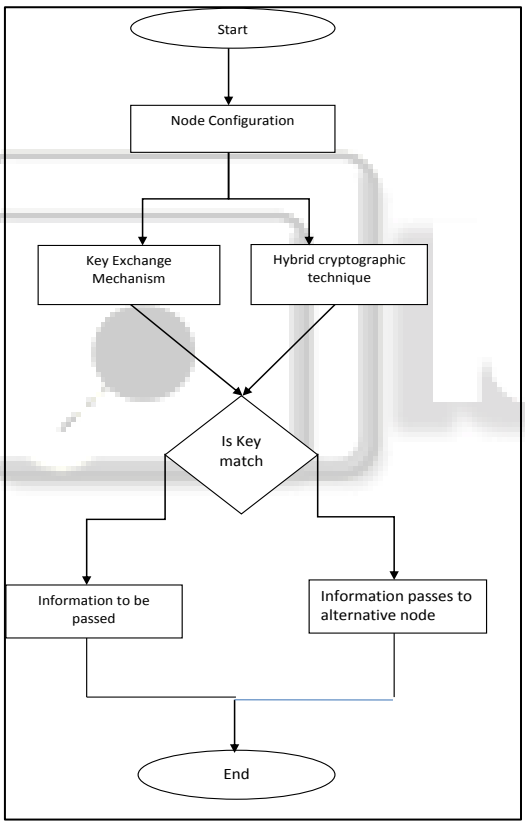


Fig. 2: Data Flow Diagram

## VI. CONCLUSION

In these paper two cryptographic techniques is used to protect our system from attackers. First method is polynomial bi-variants key; this technique gives security to the user by giving authorized key which can be a protecting function of users from the attackers. Second method is one way hash chain algorithm; this technique gives security to the data or packets transmits from source to destination which protecting in the way of adding hash data and wrapped key at each stage of intermediate node. This gives more security to the data. This technique is more effective and increases the network lifetime. This system gives more security to the users and will detect the attackers accurately.

## ACKNOWLEDGMENT

I extend my sincere thanks to my institution, 'K.S.R. College of Engineering' for giving me the opportunity to write a research paper. A special thanks to my Head of the Department, Dr. A. Rajiv Kannan for encouraging us and to Mr. C. Anand for his support and valuable guidance throughout this project work and makes this project as a successful one. Finally, I would like to thank authors of the various research papers that I have referred to, for the completion of this work.

## REFERENCES

[1] Tan .Z, A. Jamdagni, X. He, P. Nanda, and R.P. Liu, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis," IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, pp. 447-456, FEB 2014.

[2] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 1073-1080, June 2012.

[3] Thatte .G,U. Mitra,and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," IEEE/ACM Trans. Networking, vol. 19, no. 2, pp. 512-525, Apr. 2011.

[4] Yu .C, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649-1662, Dec. 2007.

[5] Tavallaee .M, E. Bagheri, L. Wei, and A.A. Ghorbani, "A Detailed Analysis of the KDD Cup 99 Data Set," Proc. IEEE Second Int'lConf. Computational Intelligence for Security and Defense Applications, pp. 1-6, 2009.

[6] Denning .D.E, "An Intrusion-Detection Model," IEEE Trans. Software Eng., vol. TSE-13, no. 2, pp. 222-232, Feb. 1987.

[7] Garca-Teodoro .P, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges," Computers and Security, vol. 28,pp. 18-28, 2009.

[8] Hu .W, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," IEEE Trans. Systems, Man, and Cybernetics Part B, vol. 38, no. 2, pp. 577-583, Apr. 2008.

[9] Jin .S, D.S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," Pattern Recognition, vol. 40, pp. 2185- 2197, 2007

[10] Lee .K, J. Kim, K.H. Kwon, Y. Han, and S. Kim, "DDoS Attack Detection Method Using Cluster Analysis, "Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.

[11] Paxson .V, "Bro: A System for Detecting Network Intruders in Real-Time," Computer Networks, vol. 31, pp. 2435-2463, 1999.

 

[12] Stolfo .S.J, W. Fan, W. Lee, A. Prodromidis, and P.K. Chan, "Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project, "Proc. DARPA Information Survivability Conf. and Exposition (DISCEX '00),vol. 2, pp. 130-144, 2000.
[13] Tajbakhsh .A, M. Rahmati, and A. Mirzaei, "Intrusion Detection Using Fuzzy Association Rules, "Applied Soft Computing, vol. 9,no. 2, pp. 462-469, 2009.
[14] Sarasamma S. T, Q. A. Zhu, and J. Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," IEEE Trans. Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 35, no. 2, pp. 302-312, Apr. 2005.
[15] Yu .J, H. Lee, M.-S. Kim, and D. Park, "Traffic Flooding Attack Detection with SNMP MIB Using SVM," Computer Comm., vol. 31, no. 17, pp. 4212-4219, 2008.



 