ADV MATH SCI JOURNAL

Advances in Mathematics: Scientific Journal **9** (2020), no.7, 4397–4404
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.7.10 Spec. Issue on RDESTM-2020

A NEW BOOSTING CONVOLUTIONAL TECHNIQUE FOR INCREASING SECURITY IN WIRELESS SENSOR NETWORK

RACHANA NAYAK, OM PRAKASH JENA, ALOK RANJAN TRIPATHY [1], SMITA RATH, AND ALAKANANDA TRIPATHY

ABSTRACT. Wireless Sensor Network (WSN) contains a small device which is known as Sensor. These devices are also used in small-radius transmission and can execute different operations, for example data management, collection of data, data analysation and processing of data. Networks of sensors are independent systems where the sensor nodes will immediately join or exit the network at any moment. If the entry node becomes an intruder node it can control the activity of the network and can cause network protection problems that can influence transmission. Symmetric technique can not be successful for autonomous systems, and can increase the difficulty of computations. A Convolution Technique (CT) is suggested in this paper that generate security bits by using convolution code to stop malevolent attack in WSNs. Dissimilar security code is developed in different nodes. The simulation result shows that proposed approach is better as compare to other four approaches that is rate of packet loss is less, the packet overhead of this approach is less and packet delivery ratio is better as other approaches. This approach increase the network security as compare to other approach.

1. INTRODUCTION

A computer network is a collection of computers which usage a set of digital interconnected transmission protocols to share assets discovered on network nodes or supplied by them. A network is composed of more than one connected computers for resource exchange (such as CD's and printers), interchanging

[1] *corresponding author*

2010 *Mathematics Subject Classification.* 68M18.

Key words and phrases. Wireless Sensor Network, Convolution Technique, Hop Count, Packet Overhead.

files, or allowing electronic transmission. In real life example, human body is equipped with several sensors capable of collecting visual information (eye), sound (ear), smell(nose).In the proposed model, at multiple Hops convolution codes are used to generate a security code and which the node must be need to match that would like to access the information. The code can be generated by using various steps. The IPV4 header helps to stock the suggested mathematical strategy in the 32 bytes protection segment. At every Hop dissimilar code are developed. The intruder node can't break the developed code until it's Time To Live(TTL), where TTL is represent the agile data packet time in outside the connection, this data packets are forwarded or retrieved inside the specified TTL to a valid node. And malevolent nodes can be quickly identified usage the suggested technique. This system is easy and slighter complicated and is differentiate to the key approaches to distribution. The paper is organised as follows: Section 2 discusses Literature Survey, Section 3 discusses Proposed Work and in Section 4 the result analysis and Section 5 depicts the conclusion.

2. Preliminaries

Newsome et al.[1] define Sybil attack in this paper. In Sybil attack malicious node take over various identities at a time and mislead normal node to think they have a lot of neighbours. It has the capability to disturb network operational integrity. These operations are distributed storage, routing [2], and allocation of resources, aggregation of the data, violating and detecting misbehaviour. To prevent the Sybil attack, they adapted a trusted centre to confirm identification of transmission entities. Two types of methods are used in CNA identification in there [3],[4]. The network is split into several zones in [5]. (Bulls).Loading of adjacent areas will be required a equal overhead interaction and the expense of calculation. The middle node of a region assesses the confidence level of cantered on sequential theories, adjacent zones submit them to a sink. Thaile et al.[3] represent a node-based confidence method applied by a sink program certificate to validate every individually entrusted node which can track malevolent nodes and meet EE, as its overhead transmission is O (n) only. In [6] the node collects the rate of packet drop, Packet Sending costs and waiting time to access the confidence values of the nodes around it. Conti et al.[7] suggested the Randomised, Secure and Distributed Protocol (RED) to identify duplication node attacks in a WSN stationery.

3. Proposed Work: The Convolution Coding Approach

This proposed model represent a model for security which is known as the convolutions technique (CT). The security code is generated by the usage of convolution approach to deter malevolent attacks on WSN. A security code depended on the digital encoding scheme (that is Convolution Coding Approach) is produced in this thesis. At first, security bits can be chose according to the demand of the network. When the security bits are selected, the Convolution Code is utilized using the EX-OR operation on the starting security bits to complete the security code word. This paper generates an 8-bit code at every Hop, based on the starting security bits as shown in the steps below:

Step 1: Calculation starting security bits

$$ISC = HC - 1$$

Where ISC is represented as starting security bits
HC represents C^{th} Hop Count , where the value of C=1, 2, 3, 4 ,5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
$*$ For example we calculate ISC ,If the Hop count HC= 1

ISC = HC - 1
= 1–1 = 0

(0 can be defined as 4-bit binary number system)Because 4 bits Convolution code generator is used. So ISC can be represented as
ISC= S1C S2C S3C S4C ISC= S11 S21 S31 S41 =0000
Here we are using a 4-bit convolution code generator to describe the proposed technique has shown in Fig 9 with G1C, G2C, G3C G4C equations are generated by performing the module-2 addition of the starting security bits. These are

$$G1C = S1C \oplus S2C \oplus S3C$$
$$G1C = S1C \oplus S2C$$
$$G1C = S1C$$
$$G1C = S1C \oplus S2C \oplus S3C \oplus S4C$$

Where IS1C, S2C, S3C, S4C are starting security bits at Cth Hop. G1C, G2C, G3C, G4C are known as generated bits at Cth Hop.For Hop 1, the initial security bits S11, S21, S31, S41=0000 and the generated bits G11, G21, G31, G41. So

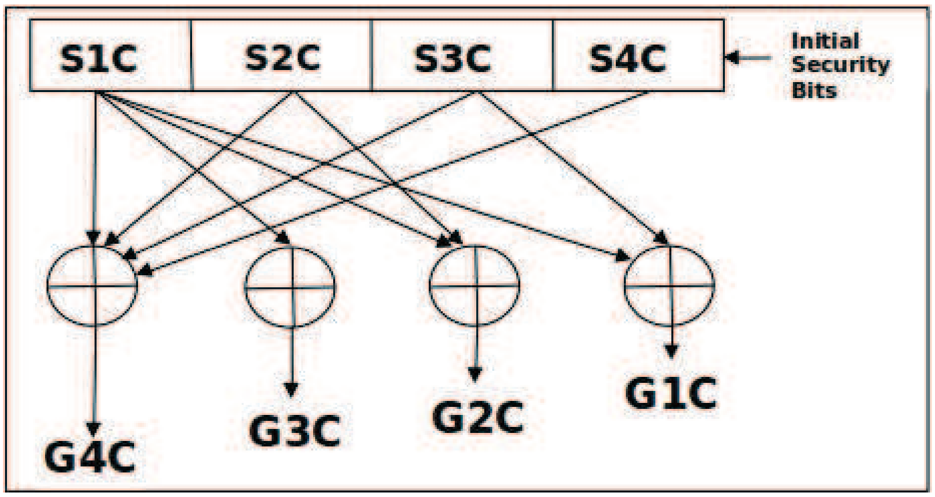


FIGURE 1. Security Code generator by using Convolution Technique

8-bit security code will be generate in the concatenation of both starting security bits and generated bits. These securities code is denote as CB.

$$CB = \prod_{i=1}^{N} SiCGi$$

Here SiC, GiC are positioned in a concatenation series N=4 are the initial bits. So at Hop 1 the value of CB= S11 S21 S31 S4 G11, G21, G31, G41=00000000 and G11, G21, G31, G41 are generated bits. This method will carry until it reaches the destination node in the network.

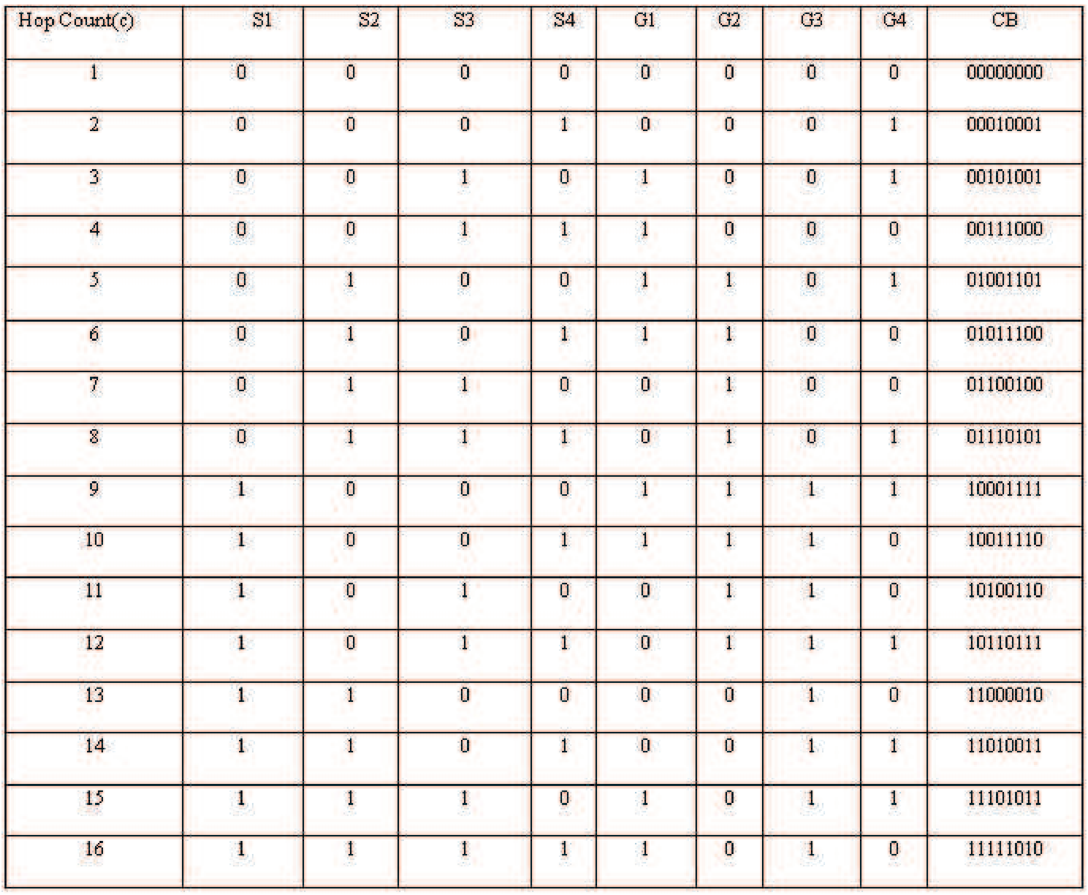
Step 2: Calculation of Hops using Proposed approach

In order to calculate hops the convolution method explained in figure 1 is used. Figure 1 shows the EX-OR operations on the starting security bits and generate G1C, G2C, G3C, G4C which is known as generated bits and Table 1 shows the 8-Bit code generation by using Convolution Technique which represent the 8-bit code with 16 Hop. Because 4 starting security bits are there and the entire hop count=24=16.

4. RESULT ANALYSIS AND DISCUSSION

The results of the proposed work are being compare with the Zhang approach[8], Ranjeetha approach [9] and Tao approach [10], Turki Approach [11]

TABLE 1. 8-Bit Code Generation using Convolution Technique



Hop Count(c)	S1	S2	S3	S4	G1	G2	G3	G4	CB
1	0	0	0	0	0	0	0	0	00000000
2	0	0	0	1	0	0	0	1	00010001
3	0	0	1	0	1	0	0	1	00101001
4	0	0	1	1	1	0	0	0	00111000
5	0	1	0	0	1	1	0	1	01001101
6	0	1	0	1	1	1	0	0	01011100
7	0	1	1	0	0	1	0	0	01100100
8	0	1	1	1	0	1	0	1	01110101
9	1	0	0	0	1	1	1	1	10001111
10	1	0	0	1	1	1	1	0	10011110
11	1	0	1	0	0	1	1	0	10100110
12	1	0	1	1	0	1	1	1	10110111
13	1	1	0	0	0	0	1	0	11000010
14	1	1	0	1	0	0	1	1	11010011
15	1	1	1	0	1	0	1	1	11101011
16	1	1	1	1	1	0	1	0	11111010

as shown in Figure 2 .These are the different approaches that give security to WSNs. Figure 2 shows the entire number of packets the receiver has sent vs the rate of Packet Loss.

The Figure 3 shows the Packet Overhead vs. Hop Count. The overhead packet for the proposed work is smaller as compared to another four approaches because key distribution is not required to every node that joins the network and updates the key at a frequent example.Table 2 depicts the packet delivery in different simulation time using all above approaches.

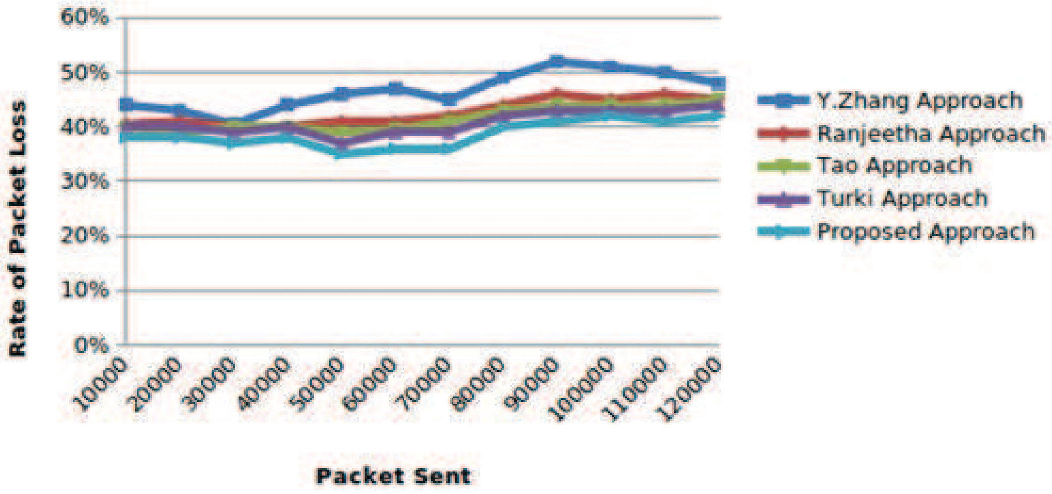


FIGURE 2. Packet Sent vs Rate of Packet Loss

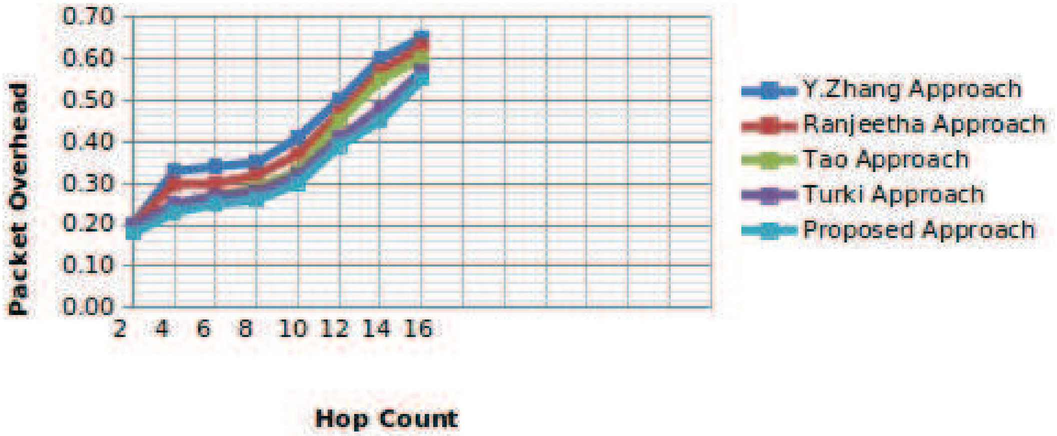
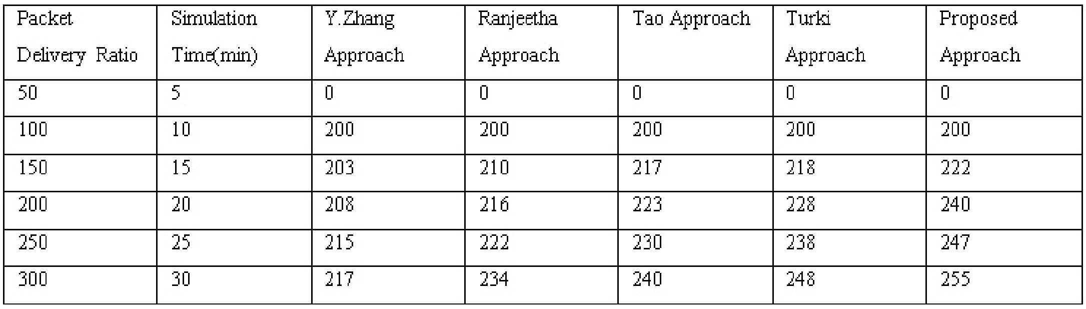


FIGURE 3. Hop count Vs. Packet Overhead

TABLE 2. Packet Delivery in Different Simulation Time



Packet Delivery Ratio	Simulation Time(min)	Y.Zhang Approach	Ranjeetha Approach	Tao Approach	Turki Approach	Proposed Approach
50	5	0	0	0	0	0
100	10	200	200	200	200	200
150	15	203	210	217	218	222
200	20	208	216	223	228	240
250	25	215	222	230	238	247
300	30	217	234	240	248	255

5. Conclusion

In wireless sensor network to provide high security data transmission convolution codes without any key distribution is used. It is a well organized approach and can be developed by using easy mathematical equation that decrease calculation energy and simply investigate node for safety data transformation from source to sink. The simulation result shows that proposed approach is better as compare to other four approach based on rate of packet loss , packet overhead and packet delivery ratio is better as compare to other approach for better security in WSN.

References

[1] J. Newsome, E. Shi, D. Song, A. Perrig: *The Sybil Attack in Sensor Networks: Analysis and Defenses*, Third International Symposium on Information Processing in Sensor Networks, (IPSN) IEEE, (2004), 259-268.

[2] C. Karlof, D. Wagner: *Secure routing in wireless sensor networks*, Attacks and countermeasures. Ad hoc networks, **1**(2-3) (2003), 293-315.

[3] M. Thaile, O. B. V. Ramanaiah: *Node compromise detection based on nodetrust in wireless sensor networks*,I 2016 International Conference on Computer Communication and Informatics (ICCCI) IEEE, (2016), 1-5, DOI: 10.1109/ICCCI.2016.7480020.

[4] R. Geetha, S. R. Anand, E. Kannan: *Fuzzy logic based compromised node detection and revocation in clustered wireless sensor networks*, International Conference on Information Communication and Embedded Systems (ICICES2014), IEEE, (2014), 1-6, DOI: 10.1109/ICICES.2014.7033974 .

[5] J. W. Ho, M. Wright, S. K. Das: *Fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing*, IEEE Transactions on Dependable and Secure Computing, **9**(4) (2011), 494-511.

[6] F. Liu, X. Cheng, D. Chen: *Insider attacker detection in wireless sensor networks*, In IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications,IEEE, (2007), 1937-1945, DOI: 10.1109/INFCOM.2007.225.

[7] M. Conti, R. Di Pietro, L. V. Mancini, A. Mei: *A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks*, Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing, (2007), 80-89, DOI: 10.1145/1288107.1288119.

[8] Y. Zhang, C. Wu, J. Cao, X. Li: *A secret sharing-based key management in hierarchical wireless sensor network*, International Journal of Distributed Sensor Networks, **9**(6) (2013), 406061.

[9] S. Ranjeetha, N. Renuga, R. Sharmila: *Secure zone routing protocol for MANET*, International Conference on Emerging Trends in Engineering, Science and Sustainable Technology, (ICETSST), (2017), 67-76.

[10] T. Yang, X. Xiangyang, L. Peng, L. Tonghui: *A secure routing of wireless sensor networks based on trust evaluation model*, Procedia Computer Science, **131** (2018), 1156-1163.

[11] A. T. Alghamdi: *Convolutional technique for enhancing security in wireless sensor networks against malicious nodes*, Human-centric Computing and Information Sciences, **9**(1) (2019), ID38, https://doi.org/10.1186/s13673-019-0198-1.

DEPARTMENT OF COMPUTER SCIENCE
RAVENSHAW UNIVERSITY
CUTTACK-753003, ODISHA, INDIA
Email address: rachananayak0610@gmail.com

DEPARTMENT OF COMPUTER SCIENCE
RAVENSHAW UNIVERSITY
CUTTACK-753003, ODISHA, INDIA
Email address: jena.omprakash@gmail.com

DEPARTMENT OF COMPUTER SCIENCE
RAVENSHAW UNIVERSITY
CUTTACK-753003, ODISHA, INDIA
Email address: tripathyalok@gmail.com

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SIKSHA 'O' ANUSANDHAN DEEMED TO BE UNIVERSITY
BHUBANESWAR-751030, ODISHA, INDIA
Email address: smitarath@soa.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SIKSHA 'O' ANUSANDHAN DEEMED TO BE UNIVERSITY
BHUBANESWAR-751030, ODISHA, INDIA
Email address: alakanandatripathy@soa.ac.in