SECURED ANONYMOUS DATA TRANSMISSION USING PARSER AND BI-VARIATE PASCAL VALUE FOR WIRELESS SENSOR NETWORKS

R.Nallakumar[1] **Dr.N.Sengottaiyan**[2]
[1] Department of Computer Science and Engineering, Anna University Regional Campus, Coimbatore-641047, India, nallakumar@yahoo.com
[2]Department of Computer Science and Engineering, Sri Shanmugha College of Engineering and Technology, Tiruchengode-637304, India, nsriram3999@gmail.com

Abstract: *A large scale Wireless Sensor Network (WSN) consists of numerous sensor nodes that may disperse over a wide-ranging zone. Sensor nodes are deployed for various applications. However, it is difficult to protect and monitor the nodes continuously for large scale sensor networks. Also providing security measures for each and every individual node in the network is a critical task. Anonymous Secured Data Transmission (ASDT) scheme is proposed here to hide the identities of nodes and to isolate the malicious node from the network. The main objective of the work is to detect the malicious node and to protect the data from the attackers. To identify the adversary nodes and to isolate them from the data transmission route Bottom-up parser approach is used. For secured transmission of data Bi-varitae Pascal value (BPV) method is considered. This generates a duplication route in which the source node, destination node, and intermediate nodes does not reveal their original node ID's and data ID's. Therefore secured and confidential information's can be passed over the nodes even in the presence of adversary nodes during routing. The simulation is carried out using NS2 simulator tool. The simulation parameters such as packet delivery ratio, lost ratio, throughput, delay and false node detection ratio are evaluated.*

Keywords: *Customary Class Nodes, Bottom-up parser, Bi-variate Pascal value, Wireless sensor Networks.*

1. Introduction

WSN is generally composed of large number of sensor nodes and it has features like low cost and low power consumption, and very compatible in size. The functionality of sensor networks includes sensing of environmental data and passing it the sink or Base Station. It performs limited data processing and communicates over short distances. The BS consists of sink node that is connected to the outside world.

The WSN used in several applications like monitoring the conditions of different objects or various process It includes military applications like battlefield surveillance, friendly force monitoring, ecological applications like flood and fire detection, agriculture monitoring, human physiological monitoring, vehicle theft detection, home applications etc.,

Thus applications necessitates communication in WSN should be highly secure. The main security threats in WSN are unsecured radio links and compromised sensor nodes. Some of the attacks in WSN are described below:

(i) Selective Forwarding: Malicious node stops the selective packets from forwarding it to the next node or it simply drops the packets from them. It causes denial of service for that particular node or a group of node. This attack also called as Gray Hole attack.

(ii) Sinkhole attack: It is one of the most destructive attacks that makes a compromised node more attractive to its neighbours and collects all the information through routing algorithm. It is difficult to identify or counter since routing information supplied is difficult to verify.

(iii) Sybil attack: A single malevolent node that present in several identities for confusing the geographic routing protocols in the network. This appears at multiple locations at the same time to pass false information.

(iv) Wormholes: The messages are replayed continuously between the distant nodes leading to hurried exhaustion of their energy resources. By fashioning well positioned wormholes an invader nearby to the BS can completely disrupt routing.

(v) Hello flood attacks: In order to proclaim the presence of nodes they broadcast hello messages frequently to their neighbors. However the powered attacker node can easily cheat or convince the other nodes even it was placed at some distance.

2. Related Works

Several security measures were undertaken for protecting the network from harmful effects caused by adversary nodes and due to other environmental factors. Several cryptographic keys were generated for providing security to the network.

For small sensor nodes public key cryptography is considered to be very expensive and computation complexity is too high. Public key algorithms such as RSA are not suitable in many cases as it requires high storage and longer key variables for key generation. To overcome the drawbacks of RSA a security technique named Elliptical Curve Cryptography (ECC) [1] was proposed for

their less complexity. It requires no key pre-distribution and pair wise key sharing. However if Base Station gets compromised then entire network gets collapsed and become totally unsecured.

Replication Attack in WSN Analysis and Defenses [2] heavily concentrates on an identity attack where one or more nodes dishonestly access the identity of legal node and replicated the entire WSN. This protocol gets activated whenever an adversary node tries to compromise the network by capturing the identity of legal node present in the network. Lightweight Sybil Attack Detection proposed a lightweight security scheme [3] to sense the new identities of Sybil attackers gone astray the centralized trusted third party. Sybil attackers are able to create more identity for a single node in order to launch coordinated attack. This scheme detects Sybil identities with good accuracy even in the presence of mobility of nodes. Trust evaluation based security solution [5] was proposed to provide effective trust based routing. The trust routing protocol allotted the trust values for each node in the network and the data transmit via trusted nodes. Identity-based key management Public key

A secured location estimation scheme was proposed [6] to secure the location information of the sensor nodes. This scheme consists of three interactive components such as secure key generation, two-way authentication and lightweight encryption for preventing the nodes from location based attack and man-in-the-middle attack. Trust sensing based secure routing mechanism (TSSRM) [7] was proposed with lightweight characteristics that have the ability to oppose various types of attacks simultaneously. Here the security route selection algorithm is taken based on trust degree of the node. However it is almost impossible to identify the individual node's behaviour in real conditions. Novel Privacy Technique includes EXTROUT a Route Extrapolation [8] was proposed to hide the original source and destination node pairs in order to provide stronger protection against powerful global attacker.

Trust Variable Factor (TVF) [9] was proposed to identify the selfish and malicious nodes based on the achieved trust rate of the node in the network. TVF is calculated by using residual energy of the node, number of packets sent by node and number of packets received by the node. To achieve anonymous communication [10] Anonymous Path Routing (APR) was proposed. Here the identities of all nodes are hided and the information is encrypted using pair-wise key, so that adversaries present in between the sender and receiver node cannot hack the actual information. Node Uncorrelated Pseudonym Pair-wise Mechanism (NUCPP) [11] was proposed to provide confidentiality to the nodes against passive attacks occurred during the communication between nodes. Stealthiness of node identity is through pseudonym mechanism since pseudonym transform rules gets deduced when correlated to a specific node. An Efficient Anonymous Communication Protocol (EACP) for WSN [12] was proposed to achieve anonymities for all the nodes with small overheads on computation, storage, and communication.

Authenticated Anonymous Secure Routing (AASR) [13] was proposed. Group Signature (GS) is used to authenticate the route request packet per hop, to prevent intermediate nodes from modifying the routing packet. Anonymous Location-based and Efficient Routing Protocol (ALERT) [14] was proposed for high anonymity protection. Here k-anonymity protection is used to strengthen the anonymity protection of data initiator node. An effective malicious node detection scheme [15] for adaptive data union in WSN under time-varying attacks was proposed using entropy-based trust model. Data union accuracy is improved by detecting miss detection constraints. Reliable Anonymous Secure Packet forwarding (RASP) scheme [16] was proposed to prevent traffic analysis attack and the attacks of compromised forwarding nodes. The mechanisms followed here are effective low computation and communication overhead. Statistical Source Anonymity (SSA) [17] in WSN is investigated here a quantitative measure is undertaken for SSA. The real valued samples are converted to binary codes in order to protect the data. However computational cost exceeds as well as it increases the overheads.

Anonymous Secured Data Transmission Method:

The main purpose of this ASDT is to categorize the malevolent node in the network and to neglect them from the routing path. Also it protects the data from the malicious observer the data is encrypted at the sender part and decrypted at the receiver part. In first phase the nodes present in the routing path are verified for its originality by their reputation values using grade factor calculation method. Based on left parse the MCN are identified in the network. In second phase an improved Bivariate Pascal Value based security algorithm is proposed for node encryption and decryption. The malicious observer in the network monitors these operations but it cannot identify the message that is passed overthe route. Therefore, the source node can send the confidential information during data transmission in the network with the help of Network Administrator (NA). The network structure or system model is shown in figure 1.

Phase I: Detection of CFG based Secured CCN

The nodes present in the networkare categorised into malevolent and customary class. Malevolent nodes are selfish behaviour nodes and customary nodes perform normal operations. These nodes are categorised on behalf of trust or reputation values of each individual node that is determined based on the grade calculation. The grade factor calculation of nodes includes their energy level and the energy threshold level. GH nodes fall under Customary Class Nodes (CCN) and GL nodes fall under Malevolent Class Nodes (MCN). The grade factor calculation is done based on total number of processed control messages as per required data transmissions. Gf is assumed to be '40' and it is considered as the certainty level of nodes for classification.

$$Gf_{(n)} = \frac{No.of\ RREQ\ processed_{(n)}}{No.of\ RREP\ processed_{(n)}}\ (G_L<40<G_H)$$

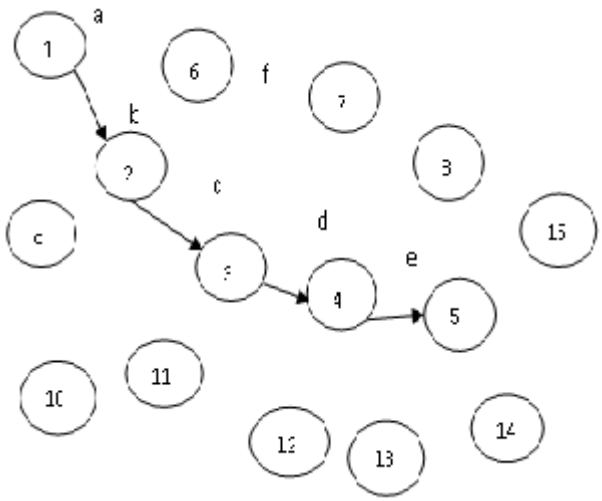

Figure 1: System Model

The customary class nodes are fallen under the category of trust nodes and Context Free Grammar (CFG) rule is applied in the left recursive production for the nodes. A leftmost derivation is derived by using the leftmost variable in each step. Considering the node '1' as a source node andthe nodes 2,3 and 4 are intermediate nodes and 5 is a Destination illustrated in the figure 1. Let p be a terminal of node 1,let q r and sare the terminals of node 2, 3 and 4 and t be the terminal of fifth node. The source and intermediate nodes are formed the leftmost derivation is given below.

Consider the grammar $G = (\{A\}, \{p, q, r, s, t\} R, A)$

$$R = \{A \to A+A, A \to A*A, A \to A-A, A \to p, A \to q, A \to r, A \to s\} \quad (1)$$

Applying CFG from the source node to its destination via intermediate nodes using left parse is given below.

$$A \overset{LM}{\Rightarrow} A+A \overset{LM}{\Rightarrow} p+A \overset{LM}{\Rightarrow} p+A*A \overset{LM}{\Rightarrow} p+q*A \overset{LM}{\Rightarrow} p+q*A-A \overset{LM}{\Rightarrow} p+q*r-A \overset{LM}{\Rightarrow} p+q*r-s\} \quad (2)$$

The routing path from source to destination among CCN is obtained using left parse based on the terminals of respectivenodes. Each node holds a string value which is given in the table. The source checks this string based on the shift reduce parser. If the source gets the empty string, the routing nodes of CCN are normal nodes else declare the routing nodes are malicious by broadcasting notification message through source node.

Applying Bottom-up Parsing Approach:

Bottom-up parser approach (Shift Reduce Parser) is applied to detect the errors quickly and accurately. The primary operations of this parser approach are move, reduce, agree to and fault or error. In a move operation, the string of the node (or) next input symbol is moved onto the top of the stack. Secondly, in reduce action; the parser recognizes the right end of the handle is at the top of the stack. It must locate the left end of the handle within the stack and decide with what non terminal to replace the handle. Thirdly, an accept action; here the parser declares successful completion of parsing. Finally error action discovers that fault has occurred if any and calls for an error recovery routine.

Load	Input key	Action
#	p+q*r-s#	Move
#p	+p*q-r#	Reduce(A→p)
#A.p	+q*r-s#	Move
#A+	q*r-#	Move
#A+q	*r-s#	Reduce(A→q)
#A+A	*r-s#	Reduce(A→A+A)
#A	*r-s#	Move
#A*	r-s$	Move
#A*r	-s#	Reduce(A→r)
#A*A	-s#	Reduce(A→A*A)
#A-	s#	Move
#A-s	#	Reduce(A→s)
#A-A	#	Reduce(A→A-A)
#A	#	Accept

Table 1: Bottom-up parsing Approach

The routing nodes are formed the string which is shown in the figure 1. The source checks the string by Bottom-up parsing approach. If the source get the empty string then the source is accept the routing path otherwise the source reject the path and identify which node is

malicious. The Bottom-up parsing approach is given in the Table 1.

Algorithm – Bottom-up parsing method:

```
Terminal = following terminal ()
repeat forever
   Source = top of stack
if act[p, terminal] = shift a then
      PUSH token
      PUSH p
token = following token()
else if act[source, token] = reduce A□p
      POP 2 * [X] symbols
      Now q = top of stack
      PUSH Aq
      PUSH goto [q,A]
      Repeat until reaches destination
Action[source, token] = "accept" then
return
else
  declare "error"
end if;
```

Phase II: Generating BPV Relay Nodes:

To protect the data transmission via malicious nodes, the source node generates a fake route so that the intermediate node will not reveal their original ID as well as the source and destination's original ID to the unauthorised users. The relay node ID is multiplied with bivariate values and sends the newly generated node ID to its next relay node. The MCN can monitor the data transmission but it cannot identify the exact source node which is sending the required information. Hence the source node sends confidential information to the destination.

Creating Fake Route:

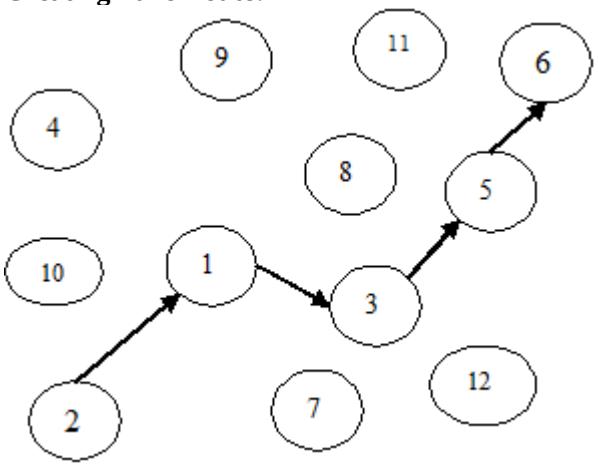

Figure 2: Fake route creation

The bivariate data is defined as the data that has two variables. These data is generated by taking the relationship between the two variables. The source node is considered as 'X' and destination node is 'Y', and the relay or intermediate node count is 'n'. The bivariate pascal value is defined as

$$\mathrm{BPV} = (X - Y)^{n}$$

The Bivariate Pascal value used to create fake route is given as (2-6)4 → {24 + 4(23)(4) + 6(22)(62) + 4(2)(63) + 64} → 16+192+864+1728+1296.

From the figure.2, it is shown that the source node is 2 and destination node is 6 and the intermediate nodes are 1, 3 and 5. The fake ID is created for each node present in the route starts from source to destination. The fake ID created for the source node is 16 and for destination is 1296, similarly fake ID for relay nodes are 192, 864 and 1728. This fake route greatly reduces the passive attacks also provides more security to the system. In addition, the fake route generation ensures that the malicious observer cannot identify the original identity of the nodes. Therefore, reduce to passive attacks during data transmission. This helps to provide more security for the data and the MCN are unable to access the data since the nodes hidden their identity and hence the origin of the node cannot be determined.

Results and Discussion:

The performance of the proposed system is examined by using the Network simulator (NS2). It is an open source programming language written in C++ and Object Oriented Tool Command Language. To estimate the proposed scheme we have assumed 50 mobile nodes, a network in an area of 1000x1500 m2. The parameters used for the simulation of the proposed scheme are tabulated in Table 1.

The protocols of proposed ASDT and the conventional SSA are compared and the performance is evaluated. The metrics such as packet delivery rate, loss rate, delay, throughput and false detection ratio are taken for the analysis.

Parameter	**Value**
Simulator	NS-2
Number of nodes	50
Traffic model	Constant Bit Rate
Channel	Wireless Channel
Channel Data Rate	100 Mbps
Transmission range	250m
Antenna	Omni-Directional Antenna
Simulation Time	100s

Table.1. Simulation Parameters

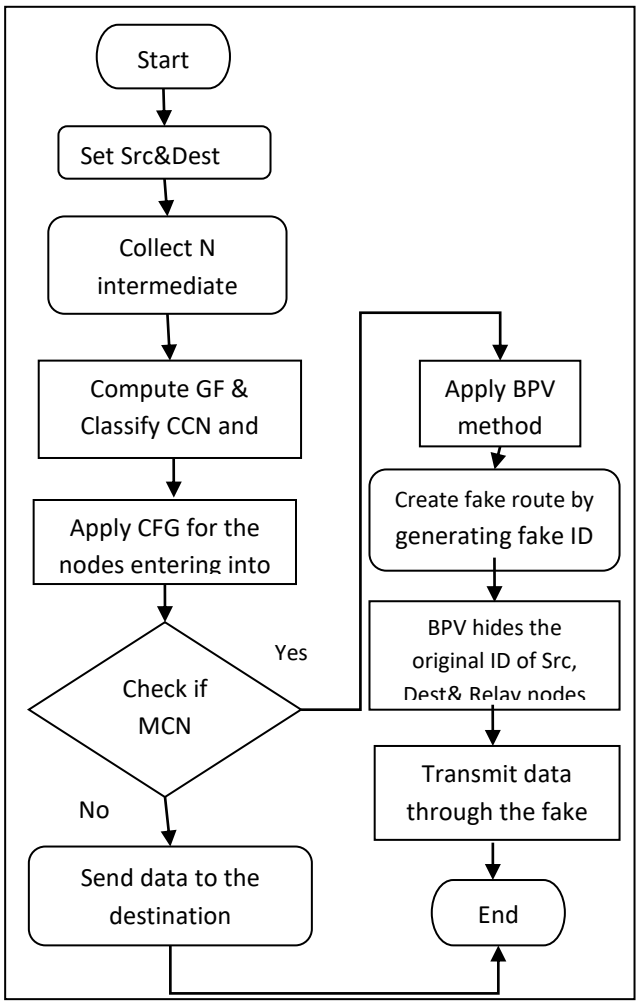

Figure 3: Flowchart of Proposed System

Packet Delivery Rate (PDR):

It is the ratio of the data packets effectively delivered to the destinations over the data packets created by the CBR sources. This metric shows the efficiency of delivering data within the network. PDR is calculated using equation (4) which is below, here 'T' represents total time taken by the data and 'n' represents the number of nodes in the network.

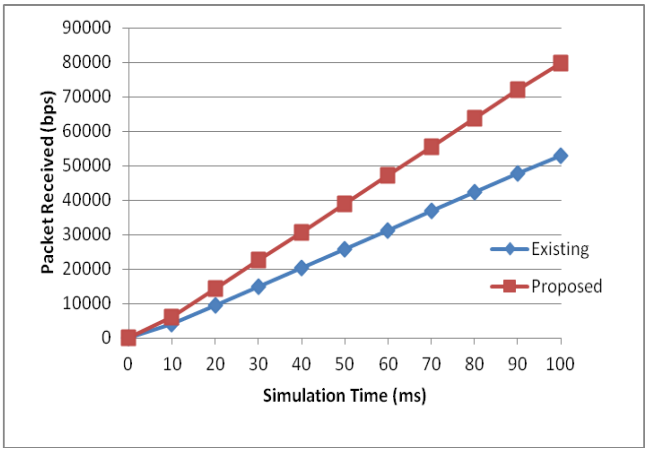

Figure 4: Packet Delivery Rate

The figure (4) shows the PDR of proposed and conventional SSA scheme. The proposed ASDT scheme achieved better PDR.

$$PDR = \frac{\sum_{0}^{n} Pkts\ Delivered}{T} \qquad (4)$$

Packet Loss Rate (PLR):

PLR is the loss ratio of packets during route unavailability and congestion scenarios. It is defined as the total number of packets lost to the total number of packets sent from source to destination node. Packet Loss Rate estimated by the equation (5).

$$PLR = \frac{\sum_{0}^{n} Pkts\ Dropped}{T} \qquad (5).$$

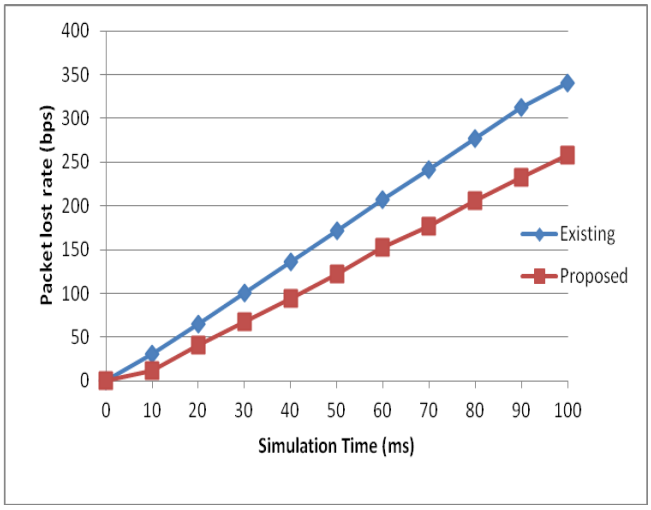

Figure 5: Packet Loss Rate

Average Delay: It is defined as the time for a packet to traverse from the source to the destination including queuing delay. This metric serves to estimate the routing policy's success of the proposed system. Where n is the number of nodes.

$$Delay = \frac{\sum_{0}^{n} Pkt\ r\ e\ cvd\ time - Pkt\ send\ time}{n} \qquad (6)$$

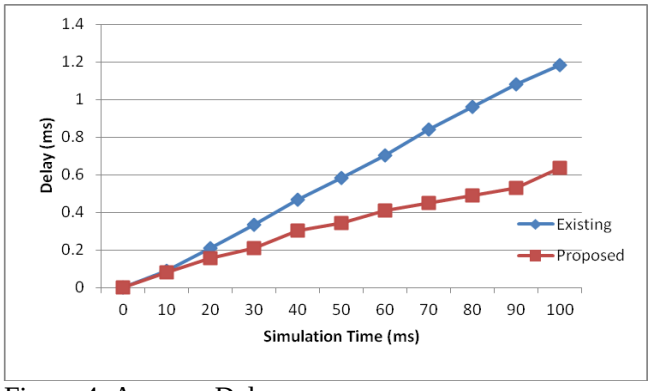

Figure 4: Average Delay

Throughput:

Throughput is defined as the rate at data is successfully transmitted for every packet sent. Generally the throughput of the network is determined by considering the overall accuracy of achievable data. The figure shows that the proposed scheme achieves better network performance compared to the SSA scheme

$$Throughput = \frac{\sum_0^n Pkts\ recvd\ (n) * Pkt\ size}{1000} \quad (7)$$

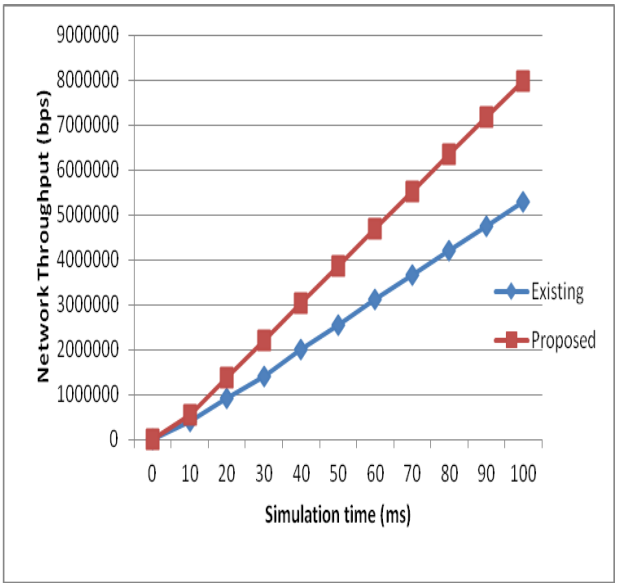

Figure 5: Throughput

Detection Ratio:

The false detection ratio for the conventional and proposed routing protocols is examined. The false detection ratio is defined as the identification of malevolent nodes with reference to the normal node.

$$False\ \det ection\ Ratio = \frac{D_{mn}}{Total_{mn}} \quad (8)$$

where D_{mn} ⟶ number of MCN is detected

T_{mn} ⟶ total number of nodes

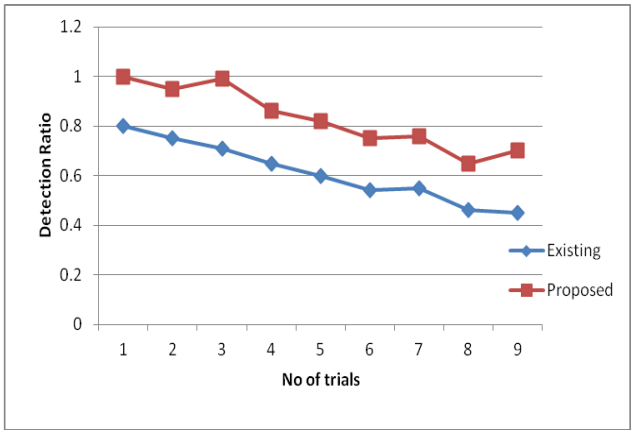

Figure 6:False Detection Ratio

Conclusion

ASDT scheme is proposed to hide the identities of nodes and to isolate the malicious node from the network. Detection of MCN and protection of data from the MCN or attackers are the main tasks of ADST. Bottom-up parser approach is used to identify the MCN nodes and to isolate them from route. For secured transmission of data Bi-Variate Pascal value method is considered. Using BVPV a route with fake node identities is created. Therefore source node, destination node, and intermediate nodes does not reveal their original node ID's and data ID's. Finally secured and confidential information's can be passed over the nodes even in the presence of MCN nodes during routing. The performance metrics is analysed for this proposed scheme using NS2 simulator tool. The simulation parameters such as packet delivery ratio, lost ratio, throughput, delay and false node detection ratio are also evaluated.

References

1. Perrig, Adrian, John Stankovic, and David Wagner. *"Security in wireless sensor networks."* Communications of the ACM 47, no. 6 (2004): 53-57.
2. Manjula, V., &Chellappan, C. (2011, January). "*The replication attack in wireless sensor networks: analysis and defences"*. In International Conference on Computer Science and Information Technology (pp. 169-178). Springer Berlin Heidelberg.
3. Abbas, S., Merabti, M., Llewellyn-Jones, D., & Kifayat, K. (2013). "*Lightweight Sybil attack detection in MANETs"*. IEEE systems journal, 7(2), 236-248.
4. P. Papadimitratos and Z. J. Haas, *"Secure routing for mobile ad hoc networks,"* in Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS '02), SanAntonio, Tex, USA, January 2002.
5. Y. Zheng, Z. Peng, and V. Teemupekka, "*Trust Evaluation Based Security Solution in Ad Hoc Networks"*, Nokia Research Centre, 2006.

6. Jokhio, Sana H., Imran Ali Jokhio, and Andrew H. Kemp. *"Light-weight framework for security-sensitive wireless sensor networks applications."* IET Wireless Sensor Systems 3, no. 4 (2013): 298-306.
7. Qin, Danyang, Songxiang Yang, Shuang Jia, Yan Zhang, Jingya Ma, and Qun Ding. *"Research on Trust Sensing based Secure Routing Mechanism for Wireless Sensor Network."* IEEE Access (2017).
8. Doomun, M. Razvi, and K. M. Soyjaudah. *"Route extrapolation for source and destination camouflage in wireless ad hoc networks."* arXiv preprint arXiv:1208.5569 (2012).
9. Talreja, Rahul, SriPradha Sathish, and Kamlesh Nenwani. *"Trust Variable Factor: A trust based method to detect misbehaving nodes in MANET."* In Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on, pp. 3238-3241. IEEE, 2016.
10. Sheu, J-P., J-R. Jiang, and Ching Tu. *"Anonymous path routing in wireless sensor networks."* In Communications, 2008. ICC'08. IEEE International Conference on, pp. 2728-2734. IEEE, 2008.
11. Yang, Guang, Guining Geng, Jing Song, Zhaohui Liu, He Han, and Xiangang Gao. "*A secure anonymous routing protocol in WSN." In Information and Automation (ICIA)*, 2013 IEEE International Conference on, pp. 415-418. IEEE, 2013.
12. Chen, Juan, Xiaojiang Du, and Binxing Fang. "*An efficient anonymous communication protocol for wireless sensor networks.*" Wireless Communications and Mobile Computing 12, no. 14 (2012): 1302-1312.
13. W. Liu and M. Yu, "*AASR: authenticated anonymous secure routing for MANETs in adversarial environments*," IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4585–4593, 2014.
14. Shen, H., & Zhao, L. (2013). *ALERT: an anonymous location-based efficient routing protocol in MANETs*. IEEE Transactions on Mobile Computing, 12(6), 1079-1093.
15. M. Abdelhakim, L. E. Lightfoot, J. Ren, and T. Li, "*Distributed detection in mobile access wireless sensor networks under byzantine attacks," IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 4, pp. 950–959, 2014.
16. Jeba, SV Annlin, and R. Suresh Kumar. "*Reliable anonymous secure packet forwarding scheme for wireless sensor networks*." Computers & Electrical Engineering 48 (2015): 405-416.
17. Alomair, Basel, Andrew Clark, Jorge Cuellar, and Radha Poovendran. "*Toward a statistical framework for source anonymity in sensor networks."* IEEE Transactions on Mobile Computing 12, no. 2 (2013): 248-260.