IFERP
connecting engineers... developing research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

DRSODA Key Management Scheme to Prevent Security Attacks in Wireless Sensor Networks

[1] D J Samatha Naidu, [2]Dr.Ande Prasad
[1]Research Scholar, [2] Principal
[1][2] Vikrama Simhapuri University, Nellore

Abstract: To address this issue of Security related attacks in wireless sensor networks, the proposed new DRSODA key management schematic approach for clustered based multi-hop scheme used for hop-by-hop dynamically distributed and centric-localized security based control for multi-hop clustered based networks which helps in security measures and also reduce the authentication problems with key maintenance overheads and also it suitable for distributed and Centralized or Hybrid related security control algorithms. New network based routing algorithms such as multi-tier data dissemination model for large scale WSN are capable of handle the overhead of mobility and topology changes according to the packet transmission in such mean-while energy constrained a lot . To address this issue, a novel data collection method called SAMRAM Enhanced Min-Max Amount shortest path(EMMASP) can be used to collect information from heterogeneous and homogenous databases networks.

Index Terms - Introduction, Related work, Proposed Methodology Work, Implementation , Simulation results.

1. INTRODUCTION

Recently, several researchers have presented clever algorithms to solve this double-counting problem. In wireless sensor network robust, scalable aggregation frame work called symmetric synopsis diffusion has been proposed for identifying duplicate aggregations using sum and count as parameters.. In this approach uses a ring topology for homogeneous networks and Complete mesh Topology uses for heterogeneous networks. In homogeneous networks node may send packets frequently without non sink failures. Where heterogonous a node may have multiple parents in the aggregation hierarchical order and each sensed value or sub-aggregate is represented by a duplicate and insensitive bitmap originator called symmetric synopsis. Furthermore , there is no provision for security related threats because most of the existing network related data aggregation algorithms are available with minor changes.

Let we notify the following issues related to the node when A compromised node might attempt to threat an existing data aggregation process by rendering several attacks like eavesdropping attacks, jamming attacks, message dropping attacks, message fabrication related attacks and etc. this paper focuses on a subclass of these attacks in which SAMRAM Enhanced Min-Max Amount shortest path(EMMASP) aims to avoid the base station to derive incorrect aggregate. By relaying a false sub-aggregate to the initial parent node, already compromised node may contribute a large amount of inconvenience to the aggregate.. As an example, during the sum and count computation a compromised node A can inject an arbitrary amount of error in estimating final Sum and count computation falsifying A's Own frequently transmitted sub aggregates. This type of attacks we referred as Falsified Sub-aggregated security attacks.

In particular, our new proposed algorithm which we call the SAMRAM EMMASP algorithm resumes the resilient computation based algorithms. It consists of two phases. The main contribution is as follows.

(1) In the first phase, the base station derives all estimated preliminary aggregated values based on minimum authentication information received from the different nodes.

(ii) In the second phase, the Base station demands and filter out of false and negative contributions of the compromised nodes from the aggregate. So the base station need more authentication information from subset aggregation of nodes.

The basic key observation needed to exploit and minimize the communication overhead related issues to verify the correctness of the final symmetric synopsis (including homogeneous networks and heterogeneous networks) the Base Station need to receive authentication messages from all of the nodes. We need finalize and examine the performance of our algorithm via both thorough theoretical analysis and extensive simulation based results. The per-node overall communication overhead in SAMRAM EMMASP algorithm is max(O(mlogA); O(mt)) where m is O(1 e2 log 1 d), A is the aggregate value, and t compromised nodes are present in the network. For heterogeneous networks Note that m items are computed in parallel fashion to result in an t=(e;d) for approximate aggregation.

II RELATED WORK

Aydayet al. proposed a slight different iterative algorithm in their main differences from the other algorithms are:

1) The ratings have a time-discount factor, so in time, their importance will fade out; and
2) The algorithm maintains a blacklist of users who are especially bad raters. proposed an iterative algorithm which beyond simply using the rating matrix, also uses the social network of users. Although the existing IF algorithms consider simple cheating behavior by adversaries, none of them take into account sophisticated malicious scenarios such as collusion attacks.

This work is also closely related to the trust and reputation systems in WSNs. Ganeriwal et al. in proposed a general reputation framework for sensor networks in which each node develops a reputation estimation for other nodes by observing its neighbors which make a trust community which employs correlation to detect faulty readings.

The main contribution of Sun et al. in is to propose a combination of trust mechanism, data aggregation, and fault tolerance to enhance data trustworthiness in Wireless Multimedia Sensor Networks (WMSNs) which considers both discrete and continuous data streams. Tang et al. in proposed a trust framework for sensor networks in cyber physical systems such as a battle-network in which the sensor nodes are employed to detect approaching enemies and send alarms to a command center. Reputation and trust concepts can be used to overcome the compromised node detection and secure data aggregation problems in WSNs.

III PROPOSED WORK

The main objective of this research work is to provide preserve against flood attacks in DTN's. The proposed approach provides node limitation over number of packets as the source node can send packets to the network at given time interval and each node also has limited transmission over the number of replicated data which are generated. To overcome the two limitations our research provides mitigate packets to avoid packet flooding attacks and replica flooding attacks, respectively. Here if any node is violated with rate limits then it will be perceived and the data traffic will be filtered. The amount of data flooded traffic can be measured through the proposed architecture. wireless sensor networks are particularly defenseless to denial of service (DoS) attacks Existing novel schemes can prevent attacks on the short term availability of a network, not for long-term availability. The most permanent denial of service attack is to entirely deplete nodes' batteries and effects on energy consumption. This is an instance of a resource depletion attack, with battery power as the resource of interest.

(i) Dos Attack

A Denial of Service (DoS) attack usually either involves attackers sending messages to feat certain susceptibilities leading to the irregularity or sending a enormous amount of regular messages quickly to a single node to run out the system resources resulting in network system failure. So long as administrators stay on top of patching vulnerabilities and optimizing the performance of business.

(ii) Sinkhole Attack

It is a service oriented attack that prevents the base station activities from obtaining complete and correct information . In sinkhole attack, a compromised node tries to fascinate the data to it from his all neighboring nodes. It may possibly happens Selective forwarding, modification or even dropping of data can be done by the sinkhole attack.

(iii) Eavesdropping Attack

Eavesdropping is a passive attack, which occurred in the Wireless sensor networks. The main aim of eavesdropping is to find some surreptitious or confidential information that should be kept top secret during the communication period of time. This confidential information may be private or public key of sender or receiver or any password based authenticated information.

(iv) Black Hole Attack

In the black hole attack, attacker uses the variety combinational type of routing protocols to advertise itself as having the best path to the node whose packets it want to intercept. For example An attacker A uses the hidden-hop flooding based protocol for listing the request for a route from the initiator, then attacker creates its own message and reply message he has the shortest path to the receiver . As this message from the attacker reached to the initiator before the reply from the actual node, then initiator assume that it is the shortest path to the receiver. So that a fake route is created by attacker A. Now it is easiest job for attacker A to grab all messages transmitted between sender and receiver.

(v) Vampire Attacks

Vampire Attacks, that ditch the life from networks nodes. Once the attacker has been able to insert himself between the communications node, then attacker may able to do anything with the packet which is send by the initiator for the receiver.
Do not interrupt immediate availability, but rather work over time to entirely disable a network.

DRSODA Key Management Scheme Here three primary contributions

• First, evaluate the susceptibilities of existing protocols to routing layer battery exhaustion attacks.

• Second, shows performance of each network and compare with simulation results by calculating the energy conservation performance of several representative protocols in the presence of a single Vampire.

• Third, modifies an existing wireless sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

The security attacks like jamming attacks and denial of service attacks in connection oriented networks are frequently characterized by amplification, e.g., use 1 minute of its own CPU time to cause the victim to use 10 minutes. Cumulative energy of an entire network, amplification attacks are always possible, given that an SAMRAM adversary can compose and send messages which are processed by each node along the message path. So, the act of sending a message is in itself an act of amplification, leading to resource exhaustion. Other attack called vampire attack as the configuration and transmission of a message that causes more energy conservation to be consumed by the network than if an honest node frequently transmits messages of identical size to the same destination, although using different packet headers.

According to the simulation results the performance can be counted. When Count is computed, A = N where N is the total number of nodes in the group of network. when Sum is computed, O(logA) = O(logN) + O(log v) where v is a single node's maximum value. An existing algorithm incurs O(N) communication overhead in the worst case, which is much higher than ours given t <<N, and the unit of sensed values are such that log(v) << N. Furthermore, our algorithm incurs O(1) latency while the other existing algorithm takes O(logN) latency whereas both the algorithms (i.e. ours and) essentially incur the same communication overhead to ensure the same approximation error guarantee.

IV PROPOSED METHODOLOGY WORK

- Node creation and packet splitting
- Trusted Authority
- Packet flood detection
- Claim Detection
- Performance Evaluation

a) Node Creation and Packet Splitting

That every packet generated by nodes is unique. This can be implemented by including the source node ID and a locally unique sequence number, which is assigned by the source for this packet; we assume that each packet has a lifetime. The packet becomes meaningless after its lifetime ends and will be discarded.

b) Activities of the Phases

In this process, the sample network formation is created.
1. The dynamic network formation is based on node creation and node connection. The node creation is based on set of node deployment.
2. To study the problem of transmitting a large amount of data packets over paths of possibly many hops, and seek optimal ways of splitting the packets into a large number of packets over multiple paths, each with different operational parameters over its hops, to minimize the end-to-end delay.
3. To calculate delay we consists primarily of random queuing delay and transmission delay at each intermediate hops.
4. The file which is to be transfer is to be selected & it is splatted into number of packets for data transmission.

c) Trusted Authority

When a user joins the network, they requests for a rate limit from a trusted authority which acts as the network operator. In the request, this user specifies an appropriate value of L based on prediction of her traffic demand. If the trusted authority approves this request, it issues a rate limit certificate to this user, which can be used by the user to prove to other nodes the legitimacy of her rate limit. Each node has a rate limit certificate obtained from a trusted authority. The certificate includes the node's ID, its approved rate limit L, the validation time of this certificate and the trusted authority's signature. The rate limit certificate can be merged into the public key certificate or stand alone.

d) Activities of the method

When a user joins the network, the user requests for a rate limit from a trusted authority which acts as the network operator.

In the request, this user specifies an appropriate value of L based on prediction of user file size. If the trusted authority approves this request, it issues a rate limit certificate to this user, which can be used by the user to prove to other nodes the legitimacy of her rate limit. To prevent users from requesting unreasonably large rate limits. The request and approval of rate limit may be done offline. The flexibility of rate limit leaves legitimate users' usage of the network unhindered. So that the.

e) Packet flood detection method

To detect the attackers that violate their rate limit L, we must count the number of unique packets that each node as a source has generated and sent to the network in the current interval. However, since the node may send its packets to any node it contacts at any time and place, no other node can monitor all of its sending activities. The node's rate limit certificate is also attached to the packet, such that other nodes receiving the packet can learn its authorized rate limit L.

f) Claim Détection

P-claim is added by the source and transmette to latté hop Along with the packet. T-claim is generated and processed hop-by-hop. Specifically, the source generates a T-claim and appends it to the packet. When the first hop receives this packet, it peels off the T-claim; when it forwards the packet out, it appends a new T-claim to the packet. This process continues in later hops. Each hop keeps the P-claim of the source and the T-claim of its previous hop to detect attacks.

g) Activities of the Method

Claim-carry-and-check can also be used to detect the attacker that forwards a buffered packet more times than its limit l. Specifically, when the source node of a packet or an intermediate hop transmits the packet to its next hop, it claims a transmission count which means the number of times it has transmitted this packet (including the current transmission). Thus, if an attacker wants to transmit the packet more than l times, it must claim a false count which has been used before. Similarly as in packet flood attacks, the attacker can be detected.

h) Assessment

• In this module, the performance of the algorithm is evaluated by using Graph representation. This shows that the proposed framework is able to adapt to changes in time and cost parameter values while the other approaches cannot. The performance gap between the proposed framework and other approaches is at the high level compare to other approaches. It provides better flexibility in the query processing process.

ADVANTAGES

- ➢ We provide a thorough empirical evaluation of effectiveness and efficiency of our proposed aggregation method. The results show that our method provides both higher accuracy and better collusion resistance than the existing methods.
- ➢ To the best of our knowledge, no existing work addresses on false data injection for a number of simple attack scenarios, in the case of a collusion attack by compromised nodes in a manner which employs high level knowledge about data aggregation algorithm used.

DRSODA Key Management Scheme working procedure consists following way:

1. Service Provider

In this ,the Service Provider using DRSODA key management Scheme dynamically selects the path and calculates the shortest path to Destination, The shortest-path routing over the Internet BGP-based router. The Service provider browses the required data packets and uploads their data files to the Specified End User (A, B, C, D) and with their DIP (Destination IP) of End User.

2. Router

The Router is responsible to route the data packets to the specified destination, the DRSODA key management Scheme is the set of the shortest physical paths simplifies the execution of this system, and finding a minimal path to the destination using routing, one can perform routing via shortest paths, the router is also responsible for Assigning the cost and also can view the cost of nodes with their tags From the node (from), To the node (to) and the cost. While the router is routing the path, if any attackers found then it will be localized using choke packet filtering algorithm. The attackers may be false injected data or IP spoofing attackers.

3. Secure Aggregation Techniques

Several secure aggregation algorithms have been proposed assuming that the BS is the only aggregator node in the network. These works did not consider in network aggregation. Only recently, the research community has been paying attention to the security issues of hierarchical aggregation. The first attack-resilient hierarchical data aggregation protocol was designed in this system. However, this scheme is secure when only one malicious node is present.

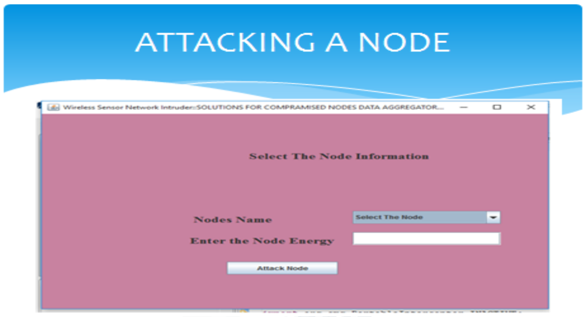
4. End User(Destination)

In this module, the End user (Node A, Node B, Node C, Node D) is responsible to receive the file from the Service Provider In the shortest-path routing between the source–destination nodes, the system consists of a one-to-many relationship. Where end User receives file from a single source to destination (Node A, Node B, Node C, Node D).

5. Attacker

Attacker is one who is injecting malicious data to the corresponding node or ip spoofing to corresponding node. The attacker can inject fake data to the particular node. After attacking the nodes, data will changed in a router.

V. SIMULATION RESULTS



ATTACKING A NODE

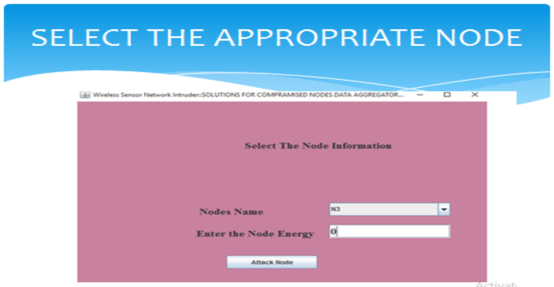
Wireless Sensor Network Intruder::SOLUTIONS FOR COMPRAMISED NODES DATA AGGREGATOR...

Select The Node Information

Nodes Name: Select The Node

Enter the Node Energy:

Fig 1: Select the Intruder run application



SELECT THE APPROPRIATE NODE

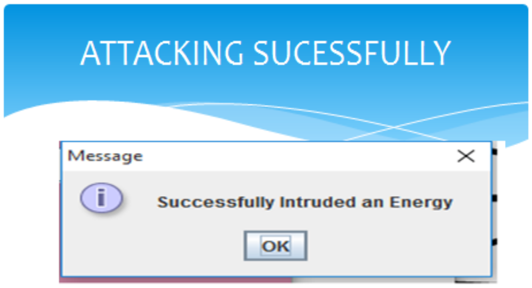
Wireless Sensor Network Intruder::SOLUTIONS FOR COMPRAMISED NODES DATA AGGREGATOR...

Select The Node Information

Nodes Name: N3

Enter the Node Energy: 0

Fig 2 . Represents attacking the appropriate node with energy ZERO

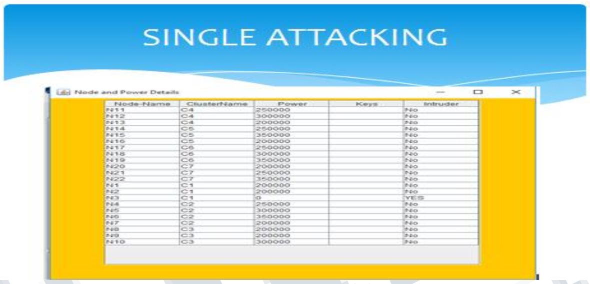


ATTACKING SUCESSFULLY

Message

Successfully Intruded an Energy

Fig 3 Node Attacked Successfully

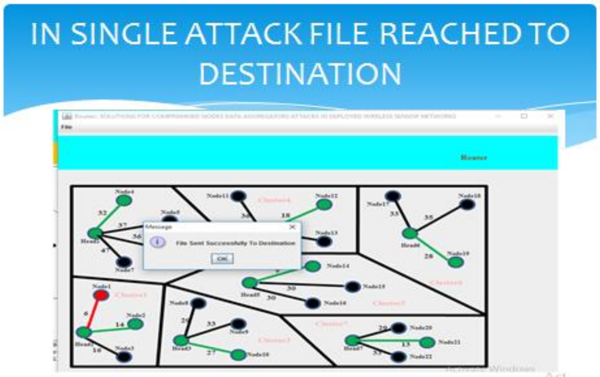


SINGLE ATTACKING

Node and Power Details

Node-Name	ClusterName	Power	Keys	Intruder
N11	C4	250000		No
N12	C4	300000		No
N13	C4	200000		No
N14	C5	250000		No
N15	C5	350000		No
N16	C5	200000		No
N17	C6	250000		No
N18	C6	300000		No
N19	C6	350000		No
N20	C7	200000		No
N21	C7	250000		No
N22	C7	350000		No
N1	C1	200000		No
N2	C1	200000		No
N3	C1	0		YES
N4	C2	250000		No
N5	C2	300000		No
N6	C2	350000		No
N7	C2	200000		No
N8	C3	200000		No
N9	C3	200000		No
N10	C3	300000		No

Fig 4 Attacking Single Node

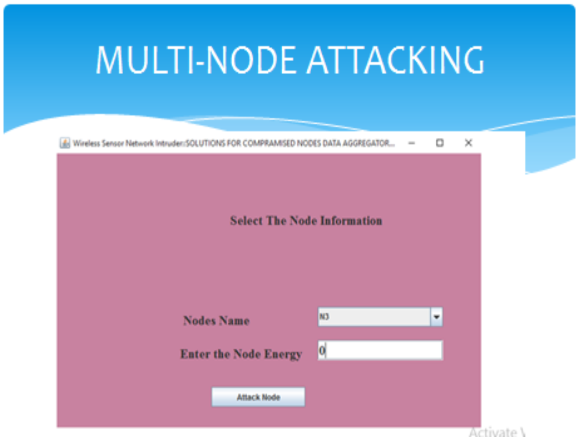


IN SINGLE ATTACK FILE REACHED TO DESTINATION

Message

File Sent Successfully To Destination

Fig 5 SINGLE-LEVEL attacking



MULTI-NODE ATTACKING

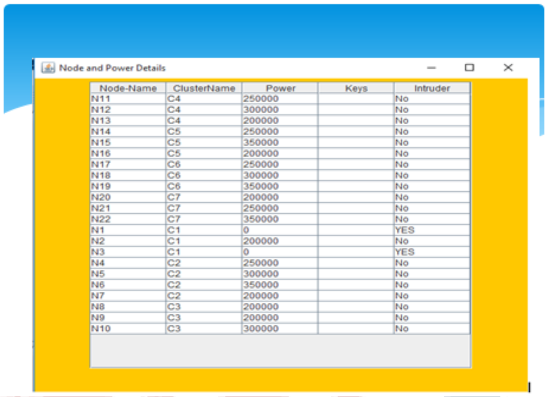
Wireless Sensor Network Intruder::SOLUTIONS FOR COMPRAMISED NODES DATA AGGREGATOR...

Select The Node Information

Nodes Name: N3

Enter the Node Energy: 0

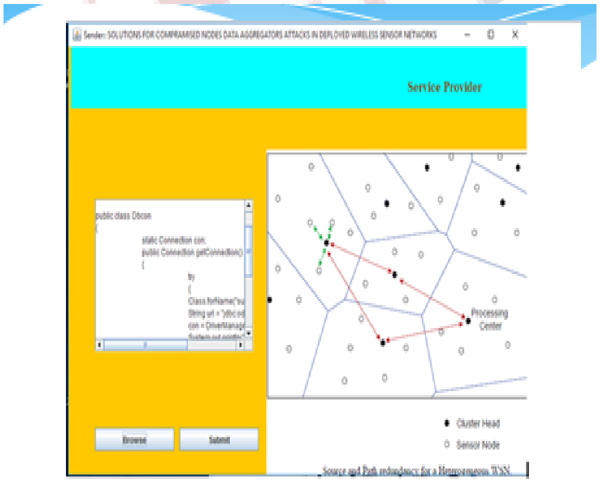
Fig 6: Multi Node attacking



Node and Power Details

Node-Name	ClusterName	Power	Keys	Intruder
N11	C4	250000		No
N12	C4	300000		No
N13	C4	200000		No
N14	C5	250000		No
N15	C5	350000		No
N16	C5	200000		No
N17	C6	250000		No
N18	C6	300000		No
N19	C6	350000		No
N20	C7	200000		No
N21	C7	250000		No
N22	C7	350000		No
N1	C1	0		YES
N2	C1	200000		No
N3	C1	0		YES
N4	C2	250000		No
N5	C2	300000		No
N6	C2	350000		No
N7	C2	200000		No
N8	C3	200000		No
N9	C3	200000		No
N10	C3	300000		No

Fig 7 Attacking DOUBLE-NODE

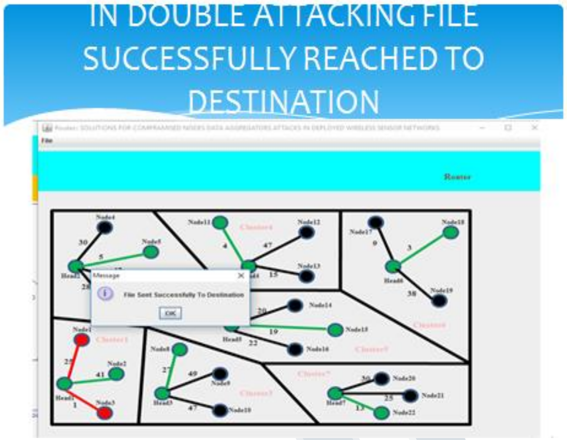


Sender: SOLUTIONS FOR COMPRAMISED NODES DATA AGGREGATORS ATTACKS IN DEPLOYED WIRELESS SENSOR NETWORKS

Service Provider

```
public class Dbcon
{
        static Connection con;
        public Connection getConnection()
        {
                try
                {
                Class.forName("su
                String url = "jdbc:od
                con = DriverManage
```

Fig 8 Packet Transmission between multiple nodes

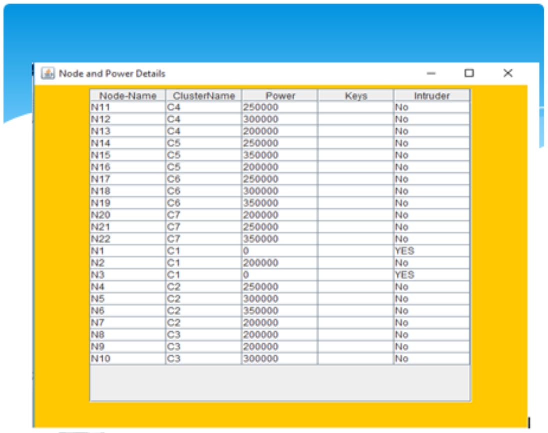


IN DOUBLE ATTACKING FILE SUCCESSFULLY REACHED TO DESTINATION

Router: SOLUTIONS FOR COMPRAMISED NODES DATA AGGREGATORS ATTACKS IN DEPLOYED WIRELESS SENSOR NETWORKS

Message: File Sent Successfully To Destination

Fig 9 MULTI-LEVEL attacking



Node and Power Details

Node-Name	ClusterName	Power	Keys	Intruder
N11	C4	250000		No
N12	C4	300000		No
N13	C4	200000		No
N14	C5	250000		No
N15	C5	350000		No
N16	C5	200000		No
N17	C6	250000		No
N18	C6	300000		No
N19	C6	350000		No
N20	C7	200000		No
N21	C7	250000		No
N22	C7	350000		No
N1	C1	0		YES
N2	C1	200000		No
N3	C1	0		YES
N4	C2	250000		No
N5	C2	300000		No
N6	C2	350000		No
N7	C2	200000		No
N8	C3	200000		No
N9	C3	200000		No
N10	C3	300000		No

Fig 10 finalized attack free packets transmitted destination successfully.

VI CONCLUSION

In this paper, an enhanced model is designed for restricting and controlling various selective attacks in Wireless sensor networks. It require further to enhance the resource and system processing to be reduced in transmitting huge data, In the current functionality the process have been checked and implemented for textual data, It require to design an enhanced model for providing security in all types of data and also design system levels to utilized the resources in a effective manner. In future work, It will investigate whether proposed approach can protect against compromised aggregators. It also plan to implement proposed approach in a deployed sensor network.

ACKNOWLEDGMENT

We are thankful for all referenced authors cited below.

REFERENCES

[1] Ramkishor Kourav, Prof. Pankaj Rechariya; Probability Based Clustering For Efficient Energy Conservation Routing in Sensor Network. International Journal of Scientific Progress And Research (IJSPR), Vol. 28, No. 02, Pages 80-83, 2016, ISSN: 2349-4689.

[2] Ramkishor Kourav, Prof. Pankaj Rechariya; Literature Review on Different Routing Methodologies in Wireless Sensor Networks. International Journal of Innovative Trends In Engineering (IJITE), Vol. 22, No. 01, 2016 Pages 31-36, 2016, ISSN: 2395-2946.

[3] Chand, K.K., Bharati, P.V., Ramanjaneyulu, B.S., Optimized Energy Efficient Routing Protocol for life-time improvement in Wireless Sensor Networks, Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on , vol., no., pp.345,349, 30-31 March 2012.

[4] Katiyar, V., Chand, N., Gautam, G.C., Kumar, A Improvement in LEACH protocol for large-scale wireless sensor networks, Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on , vol., no., pp.1070,1075, 23-24 March 2011.

[5] Arabi, Z., HERF: A hybrid energy efficient routing using a fuzzy method in Wireless Sensor Networks, Intelligent and Advanced Systems (ICIAS), 2010 International Conference on , vol., no., pp.1,6, 15-17 June 2010.

[6] Yanwei Wu, Xiang-yang Li, Mo Li, Wei Lou, Energy-Efficient Wake- Up Scheduling for Data Collection and Aggregation, Parallel and Distributed Systems, IEEE Transactions on , vol.21, no.2, pp.275,287, Feb. 2010.

[7] Z.A. Eu, H.P. Tan, and W.K.G. Seah. Opportunistic routing in wireless sensor networks powered by ambient energy harvesting. Computer Networks, 54(17):2943_2966, 2010.

[8] N. Pantazis, S. Nikolidakis, and D. Vergados. Energy-e_cient routing protocols in wireless sensor networks: A survey.

[9] S.K. Singh, MP Singh, and DK Singh. Routing protocols in wireless sensor networks_a survey. International Journal of Computer science and engineering Survey (IJCSES), 1(2):63_83, 2010.

[10] DA Vidhate, AK Patil, and SS Pophale. Performance evaluation of low energy adaptive clustering hierarchy protocol for wireless sensor networks.