Energy Aware Data Transaction in WSN using Secure AODV-CC

V.Bindu, Nithya.M

Abstract*: The problems of reducing energy consumption, maximizing sensor network lifetimes and attaining better performance in case of reducing transmission delay are hot research areas in the field of wireless sensor networks (WSN). Several approaches are invented to overcome these issues but still it is a wide research area. In this paper, an efficient routing algorithm, Secure Ad hoc On-demand Distance Vector – Criteria Checking (SAODV–CC) have been implemented which selects the path between source to destination based on criteria such as energy level and minimum distance. Once path is allocated transmission will takes place, and if any error occurs alternate path will be chosen for retransmission. Therefore it starts again from the source node and it consumes energy for transmission of same packet and it decreases network lifetime. In our proposed work, if any issue takes place, the previous node is taken as source and path selection takes place with respect to our criteria's. For secure data transaction RC4 security algorithm has been used. Therefore our proposed work achieves better result in energy consumption reduction and secure data transaction.

Index Terms*: Minimum energy consumption, security, AODV-CC, RC4 algorithm, By pass approach.

I. INTRODUCTION

WSN are created by a huge set (hundreds to a few thousands) of homogenous hubs with tremendous sources limitations. Individual sensor nodes are created with a capability of knowledge for signal processing and data networking. These hubs are spread generally over the zone to be observed to assemble information, process it, and exchange it to a focal hub for further preparing. However, wireless sensor networks the hubs are seriously need essential assets, for example, stockpiling, handling force, vitality and henceforth security systems utilized in customary systems are not appropriate for WSN.

1.1 Challenges in WSN:

There are several challenges are faced in wsn here discussed some of the unique challenges which need much attention to improve network performance. Stringent resources are the most important challenges should be handled by these networks. Due to its small size in nature and network lifetime are considered to be important parameter for issues. Few of major challenges are discussed below:

Energy constraints:

One of the main and biggest constraints in wsn is energy. It is the most costly asset. Where a large portion of the sensors are battery fueled and are used in regions, for example, profound backwoods, seas and so on there for energizing the hubs is a troublesome procedure. Sun oriented fueled is additionally utilized for change yet batteries are primary asset limitations. Vitality is spent both for calculation and information transmission. Transmitting a solitary piece of information requires as much as vitality in executing 800-1000 guidelines and accordingly information transmission expends the biggest lump of accessible vitality.

Memory Constraints:

In sensor nodes small amount of storage space will be available; moreover half of this storage will be utilized by resident operating system. Storing of data alone is not the purpose of memory is additionally required for putting away applications, information detected by the gadgets and for chronicle middle of the road aftereffects of handling. Therefore implementing security primitives in small storage is again a constraint.

Unreliable Communication:

Communication in WSN takes place through connectionless manner therefore loss of packet and congested network are also takes place. Likewise the communicate idea of the correspondence adds to the instability in correspondence.

Remote Management:

Sensor nodes are highly utilizes by the areas where devices are not able to deploy physically. They remain unattended and have to be activated through remotely and it is a challenging task. Also it makes these networks highly vulnerable to physical attacks.

1.2 SECURITY REQUIREMENTS:

The objective of security benefits in WSN is to shield the data and assets from assaults and mischief. The security prerequisites in WSN incorporate:

a. Availability: Even in the presences of denial of service attacks the delivery of desired services in a network assurance is availabiltiy.

Revised Manuscript Received on June 07, 2019.

V.Bindu, Department of Computer Science and Engineering, Research Scholar, V.M.K.V.Engineering College, Salem.

Dr.Nithya.M, Head of the department-Computer Science and Engineering, V.M.K.V.Engineering College, Salem

b.Authorization: information provided by nodes to a network should be obtained through authorized sensors.

c. Authentication: communication between sensor nodes should takes place with proper authentication. Hence attacker nodes cannot act as trusted node in a network.

d. Confidentiality: only authorized users alone can understand the message.

e. Integrity: data transferred from source to destination is not altered at any node by malicious intermediate nodes.

f. Non-repudiation: avoiding duplication of packets in network**.**

g. Data Freshness: ensures transaction of no old messages and recent data are transmitted**.**

h. Robustness: At the point when a few hubs are undermined the whole system ought not be undermined.

i. Self-organization: Hubs should be sufficiently adaptable to act naturally sorting out (self-ruling) and self-mending (disappointment tolerant).

j. Time Synchronization: These conventions ought not be controlled to deliver erroneous information.

The objective of this article is to reduce energy consumption of nodes thereby to increase network lifetime. However increasing network lifetime alone does not ensure performance improvement it also needs to ensure complete packet delivery between sources to destination. In section II related works of our proposed approach has been discussed. Implementation of our work and result obtained according to it has been described in section III and IV respectively.

II. RELATED WORKS

This section describes related work of our proposed work and finalize our proposed work attains better performance. List of papers are discussed below. Qin Yu et.al (2013), describes a hot region of research as of late. Remote sensor systems are normally put in mind boggling and unsafe condition without anyone guarding, so the trading of battery is badly arranged. In this manner, vitality sparing is dependably the key issue in the exploration of WSNs with the end goal to drag out the lifetime of systems. This paper advances an AODV directing convention, AODV-ECA, in light of cell automata (CA) component. AODV-ECA can lessen and balance vitality utilization to drag out the system lifetime by methods for exchanging hubs' states among resting and working.

Mohammed Aashkaarn and Purushottam Sharma (2016), presents mobile Ad hoc Networks are otherwise called Mesh Networks which are self-arranging systems of cell phones associated by remote connections. This paper proposes an improvement in an AODV convention which is an overhaul in the current AODV convention. The convention count which is gotten by Energy Efficient Ad Hoc Separation Vector tradition (EE-AODV) has updated the RREQ furthermore, RREP dealing with technique to save the imperativeness in cell telephones.

Dr. Annapurna P Patil et.al (2014) describes energy preservation is an major problem in applications, for instance, crisis and armed assignments needs essentialness successful plans. The projected process is a more up to date variety of the AODV directing convention, which handles real issues in MANETs like versatility and vitality proficiency. It is accomplished by assessing vitality estimations of the hubs and sending bundles along slightest depleted hubs way, making the system versatile in nature.

Mohamed Tekaya et.al (2010), presents remote systems comprising of a gathering of portable hubs with no settled foundation. Due to their decentralized, self-designing and dynamic nature, MANETs offer numerous favorable circumstances and are anything but difficult to introduce. Be that as it may, with this dynamic topology, portable specially appointed systems have a few difficulties like the plan of a proficient directing convention. A case for this test is stack adjusting. The multipath steering convention with load adjusting gives an answer for the clog system and expands it's ability. To consider that the utilization of various ways all the while for transmission information permits to enhance the system execution, we propose another convention LB-AOMDV (Load Balancing-AOMDV), an answer for accomplish better load adjusting instrument. The reenactment's outcome demonstrates the critical execution change of the system for the multipath directing convention with load adjusting. Mrs. Poonam Meghare and Preeti Deskhmukh (2014), discusses the vitality utilization and to maintain a strategic distance from bundle loss of remote sensor systems. Accordingly, a correspondence convention AOMDV is utilized . A Mobile Ad hoc Network is exceedingly powerful remote system that can framed without the requirement for any previous foundation in which every hub can go about as a switch. The AOMDV(Ad-hoc 0n-request Multipath Distance Vector) Routing convention. AOMDV convention is an augmentation to the AODV(Ad-hoc On-request Distance Vector) Routing convention for figuring different circle free and connection disjoints ways. AOMDV was planned basically for exceedingly powerful impromptu systems where connect disappointments and course breaks happen much of the time. It brings about more directing overheads and parcel delay than AODV yet it had a superior effectiveness with regards to number of parcel dropped and bundle conveyance. AOMDV diminishes directing overhead by decreasing the recurrence of course revelation activity.Prashant Kumar Maurya et.al (2012), presents the working and need of AODV protocol. AODV is a receptive convention: the courses are made just when they are required. It utilizes customary steering tables, one passage for every goal, and succession numbers to decide if directing data is forward-thinking and to avert steering circles. An imperative element of AODV is the support of time sensitive states in every hub: a directing passage not as of late utilized is terminated.

If there should arise an occurrence of a course is broken the neighbors can be advised. Course revelation depends on inquiry and answer cycles, and course data is put away in every single moderate hub along the course as course table passages. The accompanying control parcels are utilized: directing solicitation message (RREQ) is communicated by a hub requiring a course to another hub, steering answer message (RREP) is unicasted back to the wellspring of RREQ, and course mistake message (RERR) is sent to inform different hubs of the loss of the connection. Hi messages are utilized for recognizing and observing connects to neighbors. Meeta Singh and Sudeep Kumar (2017), discusses the primary objective of Ad-hoc on demand distance vector (AODV) protocol. This paper gives a basic audit of writing on versatile spontaneous systems and the steering conventions. This paper wills talks about the idea and qualities of versatile specially appointed systems. The highlights and grouping of the specially appointed steering conventions and clarifies the depiction of Ad-hoc on interest remove vector (AODV) convention with its systems. This paper likewise examines the connection disappointment in portable specially appointed systems and the connection state forecast is shown. Isnar Sumartono et.al (2016), describes file security is basic in keeping up the secrecy of the data, particularly touchy data that should just be known by approved people as it were. In the event that the information isn't stayed discreet, the data got may prompt unfortunate occasions and abused by gatherings that are not responsible. The most ideal way is utilized for document security is cryptography. One of the calculations utilized is RC4. During the time spent this calculation, the key created by framing the S-Box. The aftereffects of the S-Box at that point are done by XOR process with the current plain character. This investigation talks about how to perform encryption and unscrambling process utilizes the RC4 calculation to every one of the ASCII record.

III. PROPOSED SYSTEM

In this section, implementation of our proposed system has been discussed briefly. Initially path has been created between source and destination using AODV (Ad hoc on demand Distance Vector). Even though it is a single path creation our proposed method attains maximum performance by implementing by pass approach. While data is transferred from source, path allocation will be created through AODV by verifying criteria such as energy level of node, minimum distance and bandwidth. In existing methods, if any issue occurred in selected path either alternate path will be selected or retransmission will be takes place. In both case, if transaction failures, data should be transferred from source again which consumes energy and it will reduce network lifetime. If any data loss occurs in our proposed method, instead transferring data from source the previous node will act as source and path will be created with respect to our criteria condition verification. In addition to ensure secure data transaction RC4 encryption is utilized.

Path selection:

For data transaction between source to destination, path selection has been done through AODV. Hence implementation of AODV is described below. AODV creates route when there is a demand in transmitting packet to destination. Similarly created routes are maintained until it required by source. Continuous number ensures the originality of routes and ensures the loop free routing.

Routing tables:

The following details are stored in routing table, such as destination ID, next hop, destination sequence number, total number of hops, active neighbors for this route and deadline for this route table entry. Deadline is also represented as expiration time and it generally denoted as lifetime. The sum of current time and active route timeout is represented as expiration time.

Route request:

Source Address	Request ID	Source sequence No	Destination address	Destination sequence No.	Hop count

When a route is not available a route request will be transmitted and the format of route request has been shown above. RREQ is identified uniquely by the pair of (Source address, request ID) hence this request ID will be incremented each time. While receiving this request each node checks whether it already received or not. If received it will be ignored or it will be forwarded and replied with a RREP message.

Routing reply:

If a node is the destination, or has a valid route to the destination, it unicasts a route reply message (RREP) back to the source. This message has the following format. The reason one can unicast RREP back is that every node forwarding a RREQ message caches a route back to the source node.

Source address	Destination address	Destination sequence No.	Hop count	Lifetime

Criteria checking:

While creating path certain criteria's are verified such as, distance between source and destination, energy level of nodes and bandwidth.

The route between sources to destination consumes minimum energy when the distance is minimum.

$$Optimum\ route1 = \Sigma(n) \in r\ ene(v(n)) / \Sigma v \in V ene(v) \quad \ldots\ldots (1)$$

Shortest route evaluation:

$$Optimum\ route2=\Sigma(n)\in r\ dist(e(n)) / \Sigma e\in E \quad \ldots\ldots (2)$$

The calculation of minimum bandwidth consumption is as follows:

optimal route 3= $\Sigma b(n)\in r\ dist(b(n)) / \Sigma b\in E$ …… (3)

Criteria checking pseudo code has been described below:

1: Source and Destination should be chosen

2: Route discovery is initialized by source.

3: Routing packets are broadcasted to direct nodes.

4: In the Source Routing Table routing information's are updated.

5: Beacon is initialized by the source

6: Broadcast the Routing Packet to direct nodes.

7: In the network the source energy table is updated with the Energy and location information.

8: check

If(ene>= High &&dist<= Low &&hop Count<= Low) … (Eq. 1 & 2)

Select that route for Communication.

Else if (ene>= High &&dist>= high &&hop Count<= Low) … (Eq. 1)

Select that route for Communication.

Else if (ene<= Low&&dist<= Low &&hop Count<= Low t) … (Eq. 2)

Select that route for Communication

Else if (ene<=Low&&dist<=Low&&bdw<=Low) … (Eq. 3)

9: Send the periodic route discovery.

10: Send the periodic beacon message.

According to bypass approach if any occurred during transaction of data in selected path then based on demand new path will be created with respect to condition verification. Therefore previous node will be considered as source node and data transmitted to destination. Hence our system ensures reliable data delivery between sources to destination.

Secure transaction:

The above phases ensure data reliability however a system is said to be optimal it should attain maximum performance. Reliability is ensured and secure data transaction also verified by implementing secure data transaction process by RC4 encryption technique. Hence its implementation has been shown below,

RC4 is a symmetric key algorithm and represented to be stream cipher. For both encryption and decryption same algorithm will be used. The data stream are simply XORed with the key sequence generated. The key stream utilized is completely independent without any knowledge of plaintext used. It utilizes a variable length key from 1 to 256 piece to instate a 256-piece state table. The state table is utilized for resulting age of pseudo-arbitrary bits and after that to produce a pseudo-irregular stream which is XORed with the plaintext to give the ciphertext.

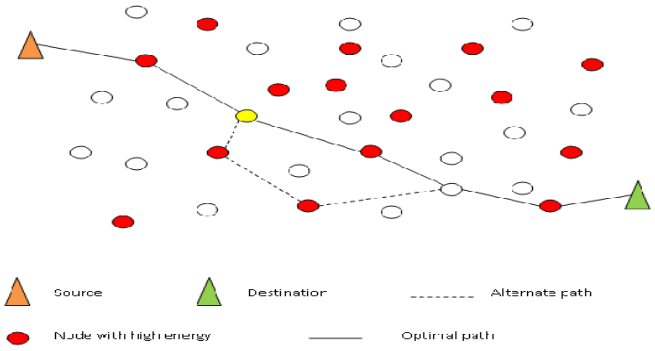

Figure 1: Architecture Diagram

The calculation can be broken into two phases: introduction, and activity. In the introduction arrange the 256-piece state table, S is populated, utilizing the key, K as a seed. When the state table is setup, it keeps on being changed in a customary example as information is scrambled. The instatement procedure can be abridged by the pseudo-code:

j = 0;

for i = 0 to 255:

S[i] = i;

for i = 0 to 255:

j = (j + S[i] + K[i]) mod 256;

swap S[i] and S[j];

The steps for RC4 encryption algorithm is as follows:

1. Get the data to be encrypted and the selected key.
2. Create two string arrays.
3. Initiate one array with numbers from 0 to 255.
4. Fill the other array with the selected key.
5. Randomize the first array depending on the array of the key.
6. Randomize the first array within itself to generate the final key stream.
7. XOR the final key stream with the data to be encrypted to give cipher text.

IV. RESULT AND DISCUSSION

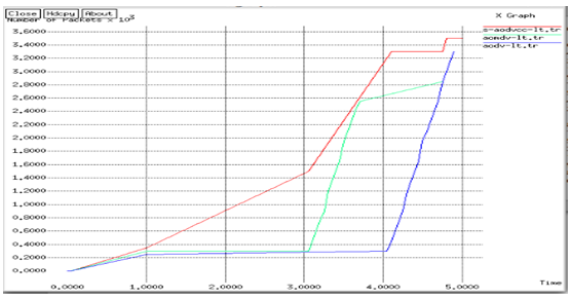

Figure 2: Network Lifetime

The above mentioned graph shows network lifetime consumption of various existing methods and our proposed method.

X axis indicates the time and y axis indicates the number of packets transmitted with respect to time. Compared to existing methods like AODV and AOMDV our method achieved better network lifetime. This could be done by minimum energy consumption while transaction of packets.

Figure 3 shows energy consumption of data with respect to time and number of packets transmission. For a particular level of data transaction AODV and AOMDV consumes different energy level and at certain point both consumes same energy level sequentially. Hence our proposed system consumes minimum energy compared to other existing methods is clearly shown below.

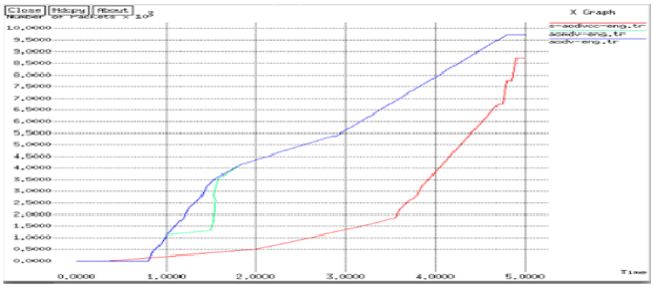

Figure 3: Energy Consumption

Figure 4 shows, reliability of our proposed system. In general reliability is measured by number of packets delivered from source to destination. Here, our proposed system achieves maximum delivery ratio compared to other existing methods. In addition it achieves maximum delivery and reduces loss of data.

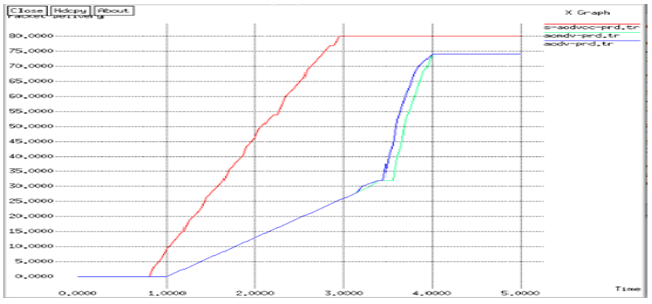

Figure 4: Packet Delivery Ratio

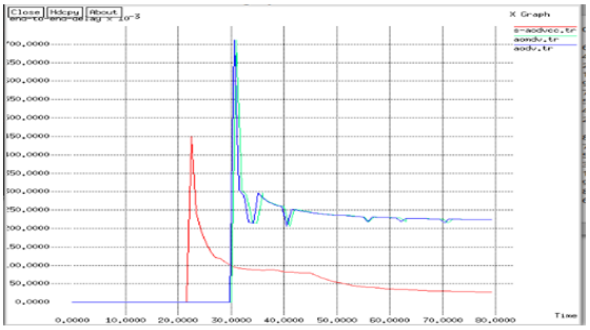

Figure 5: End To End Delay

Figure 5 shows, end to end delay of data from source to destination. End-to-end delay or one-way delay (OWD) refers to the time taken for a packet to be transmitted across a network from source to destination. If delay occurs during packet transaction then it could not considered as a optimal one. Hence our system shows minimum dealy ratio compared to existing methods.

V. CONCLUSION

Enhancing network lifetime is a major research area in WSN. In this paper we have achieved both reliability and secure data transaction in focus of enhancing network lifetime. Our proposed secure AODV-CC method achieves efficient data transaction between source to destination with condition checking such as minimum distance, high energy level and bandwidth consumption. With respect to on demand need of path creation these criteria were checked to ensure reliable data delivery. Similarly, a system which achieves reliable delivery with minimum energy consumption does not ensure best performance. Secure data transaction also should be ensured during transaction hence this can be achieved by implemented RC4 encryption technique. Hence we can conclude that our system achieves better reliability and secure data transaction with enhancing network life time. Compared to existing method our proposed achieves better result in all required parameters.

REFERENCES

1. Yu, Q., An, N., Wang, T., Leng, S., & Mao, Y. (2013). AODV-ECA: Energy-efficient AODV routing protocol using cellular automata in wireless sensor networks. 2013 International Conference on Communications, Circuits and Systems (ICCCAS).
2. Aashkaar, M., & Sharma, P. (2016). Enhanced energy efficient AODV routing protocol for MANET. 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS).
3. Patil, A. P., Chandan, B. V., Aparna, S., Greeshma, R., & Akshatha, H. P. (2014). An improved energy efficient AODV routing protocol for MANETs. 2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN).
4. M. Tekaya, N. Tabbane, and S. Tabbane, ``Multipath routing mechanism with load balancing in ad hoc network," in *Proc. Int. Conf. Comput. Eng. Syst. (ICCES)*, Nov. 2010, pp. 67_72.
5. Mrs. Poonam Meghare, Prof. Preeti Deskhmukh, "Packet Forwarding using AOMDV Algorithm in WSN" International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 3, Issue 5, May 2014.
6. Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts, Mahendra Srivastava, "An Overview of AODV Routing Protocol" International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.3, May-June 2012 pp-728-732.
7. Meeta Singh, "A Survey: Ad-hoc on Demand Distance Vector (AODV) Protocol" International Journal of Computer Applications (0975 – 8887) Volume 161 – No 1, March 2017.
8. Isnar Sumartono, Andysah Putera Utama Siahaan, Nova Mayasari, "An Overview of the RC4 Algorithm" IOSR Journal of Computer Engineering (IOSR-JCE) Volume 18, Issue 6, Ver. IV (Nov.-Dec. 2016).