Secure And Energy Efficient Detection of Wormhole Attack in WSN Using Hybrid Approach

P Gnanapriya,

M.E (Computer Science and Engineering) Final year, Mahendra Engineering College, Namakkal.

Dr.P.Ramya, M.Tech.,Ph.D.,

Associate Professor, Department of Computer Science and Engineering,

Mahendra Engineering College, Namakkal -637 503

ABSTRACT:

In wireless sensor network, secure data transaction from source to destination is a major goal. The goal to be achieved in WSN is to increase network lifetime and to achieve efficient data transaction among nodes. Similarly during data transaction there is a possibility for various attacks and it leads to data loss. In our work most important attack like wormhole attack is focused and efficient method has been proposed. Here initially path selection has been done through Energy Efficient Ad hoc on demand Multipath Distance Vector (EE-AOMDV). This selects optimal path between source and destination. The nodes to be selected for transaction is attack free nodes hence wormhole attacker nodes should be detected efficiently through hybrid approach of watchdog and RTT. Through, this approach wormhole attack has been detected and that particular node will be avoided for further transaction. To protect our data from other forms of attack in our proposed work packets are encrypted and transmitted through the path which has been verified from wormhole attack and considered to be reliable transaction. Hence our proposed work obtains better performance compared to other existing approaches like AODV and HEER.

Keywords: EE-AOMDV, hybrid approach, wormhole attack, network lifetime and RC4.

I.INTRODUCTION

WSN is an interfacing of hubs from some to a few hundreds or even thousands in which every hub is related with one sensor or a few sensors. Homogeneous or heterogeneous sensor hubs are utilized in WSN. Calculations are constrained in sensor organizes a few instances of calculations are hub power, quality of sign and support size. WSN has numerous applications that are Area checking, Healthcare observing, Environmental or earth detecting, and Industrial observing.

In WSNs directing is ordered into level based steering, progressive based directing, and area put together steering with respect to the structure of system as a rule. Each hub is traditionally alloted equivalent jobs or usefulness in level based directing. On the other hand, hubs will assume unique jobs in the system in progressive based steering. Sensor hubs' positions are persecuted to course information in the system in area based directing.

In course disclosure a significant measure of vitality is used and receptive conventions arrangement. Hubs send information to internal hub, are gathered in helpful directing, and may likewise use in extra handling, subsequently it diminishes course cost as far as vitality use. A ton of different conventions rely upon position data and timing.

Major issues in sensors:

- Limited memory and storage
- Energy consumption

ISSUES IN WSN:

Jamming

It is caused because of obstruction with the radio frequencies of the system's gadgets which is an assault on the accessibility of the sensor arrange. It is unique in relation to typical radio engendering in how it is undesirable and problematic, consequently bringing about forswearing of-administration conditions.

Tampering

It is likewise called hub catching in which a hub is undermined, it is anything but difficult to perform and is truly destructive. Altering is truly changing and devastating sensors hubs.

Collision:

It is caused in interface layer that handles neighbor-to-neighbor correspondence alongside channel assertion. Whole bundle can be upset if an enemy can create impacts of even piece of a transmission, CRC confound and potentially require retransmission can be brought about by a solitary piece blunder.

Exhaustion:

Exhaustion of a system's battery force can be incited by a cross examination assault. An undermined hub could over and again send along these lines expending the battery power more than required.

Wormhole attack

It is caused because of arrangement of a low-idleness interface that is shaped with the goal that bundles can venture out from one to the opposite end quicker than regularly through a multi-jump course. The wormhole assault is a risk against the directing convention and is trying to distinguish and forestall. Right now assault, an enemy can persuade the far off hubs that are just a couple of jumps away through the wormhole creating turmoil in the system steering components.

Contribution of the paper:

- To increase network lifetime by reducing energy consumption of sensor nodes.
- To transfer data in secure way without any attacks.
- To protect from other common forms of attack encryption method is used.
- By utilizing energy efficient path selection algorithm energy consumption will be reduced.

II.LITEREATURE SURVEY

Muhammad Imran et.al(2015), states that systems have greater security dangers because of absence of main issue of control when contrasted with fixed systems. Wormhole assault is one of the most extreme steering assaults, which is propelled by two conniving hubs by setting up a private channel between them. This paper introduced the highlights that could be utilized to recognize the wormhole assault. These highlights are talked about in detail with their advantages and disadvantages. The potential confinements of Intrusion Detection Systems (IDSs) are likewise talked about. This work gives a premise to construct an effective IDS to recognize wormhole assaults in MANETs. As indicated by our examination, the methods dependent on course demand (RREQ) or jump tally would be superior to anything different systems to distinguish wormhole assaults.

Ajay Prakash Raiet.al (2012), presents wormhole assault recognition in WSN. In MANET hubs which are inside the scope of one another can associate straightforwardly where as hubs which are not in the region of one another depend on the middle hub for correspondence. Correspondence in the system relies upon the trust upon one another. In wormhole assaults, one malignant hub burrows parcels from its area to the next vindictive hub. Such wormhole assaults bring about a bogus course with less. On the off chance that source hub picks this phony course, malevolent hubs have the choice of conveying the bundles or dropping them. It is hard to recognize wormhole assaults on the grounds that noxious hubs mimic real hubs The wormhole assault is conceivable regardless of whether the assailant has not bargained any hosts and regardless of whether all correspondence gives validness and classification.

Louazani Ahmed et.al (2014), describes identifying and maintaining a strategic distance from wormhole assault. CL-MAC convention is the aftereffect of our past research works for which the security viewpoints have not been thought about during its plan arrange. To officially demonstrate the significance of the proposed plot, we give a hypothetical report dependent on Time Petri Net to investigate some significant properties identified with the staggering impact of the wormhole assault and its countermeasure on the CL-MAC activities.

Soorya V Nair and Shijin Knox G U (2019), describes energy consumption is treated as one principle downside in MANET. This paper manages a technique to improve the vitality effectiveness and system lifetime in portable impromptu system by utilizing a multipath directing convention AOMDV. The proposed EE AOMDV utilizes vitality limits to choose vitality effective ways from accessible ways at the hour of directing. When AOMDV is contrasted and EE AOMDV, the outcomes show that the proposed EE AOMDV is more vitality productive than AOMDV. The parameters utilized for the examination are vitality utilization of the system and lifetime of the system by shifting hub speed, information rate and reproduction time.

Mary Cindy Ah Kioon et.al (2015), discuss about MD5 encryption calculation. Hashing calculations are ordinarily used to change over passwords into hashes which hypothetically can't be deciphered. This paper investigations the security dangers of the hashing calculation MD5 in secret phrase stockpiling and examines various arrangements, for example, salts and iterative hashing. We propose another way to deal with utilizing MD5 in secret phrase stockpiling by utilizing outer data, a determined salt and an irregular key to scramble the secret phrase before the MD5 figuring. We recommend utilizing key extending to make the hash computation increasingly slow XOR figure to make the last hash esteem difficult to discover in any standard rainbow table.

Mrs. C. Gayathri and Dr.R. Vadivel (2017) presents Watchdog Mechanism is a key structure squares to many trust frameworks that are intended for making sure about Mobile Ad-hoc Networks. Guard dog Technique is one of the Intrusion Detection Technique in specially appointed systems. The above Watchdog Methods it speak to with interruption identification framework being a significant job of portable impromptu system. Right now the various sorts of Watchdog Mechanism included the noxious hub recognition process. . It appears that the simpler for the clients to comprehend the Watchdog Mechanism.

III.PROPOSED METHODOLGY

In proposed framework, at first way has been chosen dependent on EE-AODV calculation. Here way is set up dependent on request and it permits making multipath between source to goal. EE-AOMDV checks the Energy/Distance proportion of every way accessible in the system. In view of interest of specific information transmission way has been apportioned and transmission of parcels were happens. Here, the identification of wormhole assault is a troublesome procedure. To recognize in an exact manner a half and half methodology has been used that is a mix of guard dog and RTT. Through this methodology wormhole assailants has been precisely and productively distinguished and disengaged from our system and does excluded from further exchange. Thus this will guarantee secure information exchange and diminishes vitality utilization if there should arise an occurrence of retransmission, parcel misfortune and deferral in conveyance. Anyway guaranteeing security can be accomplished through executing cryptography calculation here the issue confronted is it will deplete the battery of sensor hubs rapidly. In our proposed work lightweight cryptography calculation has been actualized through MD5. This gives proficient and make sure about information exchange without devouring more vitality in organize.

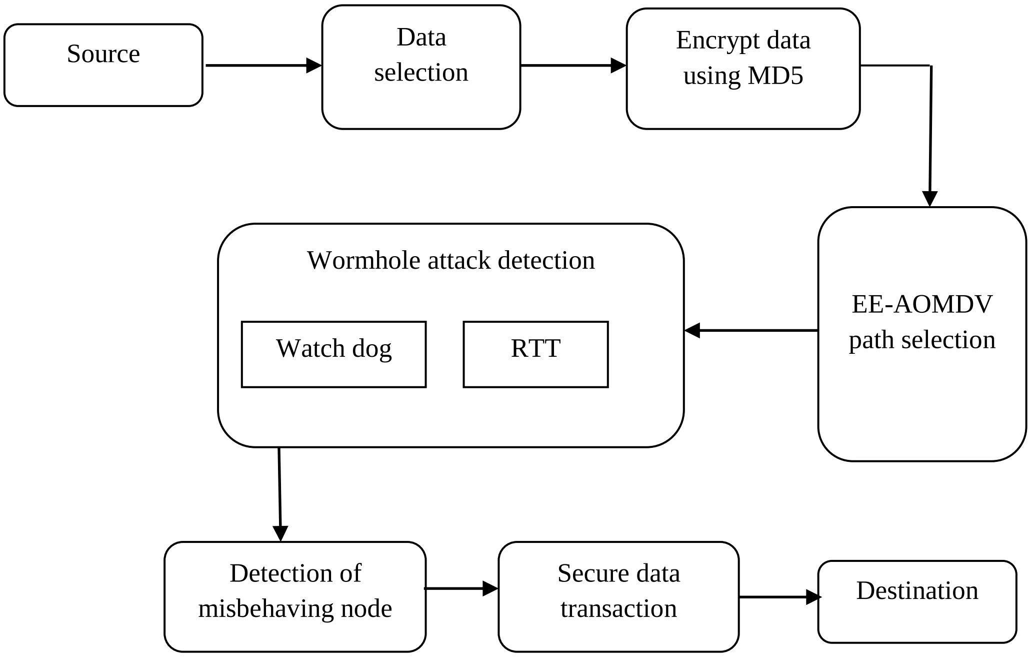

Figure 1: Working flow of proposed system

EE-AOMDV route selection

EE-AOMDV utilizes vitality limits for choosing the hubs with high remaining vitality. Right now, utilization can be diminished for the entire system. The proposed EE AOMDV convention intends to choose ways with high residual vitality and less vitality use. This maintains a strategic distance from interface disappointments caused because of the exhaustion of hubs vitality and subsequently expanding the lifetime of the system and improves the vitality execution in MANETs. The calculation figures out which of the gadgets in the system should be chosen in a specific course. At the point when we select cell phones without thinking of it as' outstanding vitality level while choosing the courses will leave a lopsided vitality level in the whole system.

Algorithm 1:

1) Select source and goal for directing

2) Source hub begins course disclosure process

3) During course upkeep every hub will checks its residual vitality level with a limit esteem (high1)

4) For each hub in the way if remaining vitality > high1 && hopcount < minimum_hopcount select that way for correspondence in the system

5) Else if select way with most limited separation and utilize that way for correspondence.

6) Send the intermittent course revelation

The energy consumption rate between two time slots can be

calculated using Algorithm 2[2].

Algorithm 2:

1) $\text{Energy}_{\text{time1}}$ and $\text{Energy}_{\text{time2}}$ are the remaining energies at time1 and time 2

2) for each hello time interval, calculate

3) Energy Consumption rate = $((\text{Energy}_{\text{time2}} - \text{Energy}_{\text{time1}}) / \text{Energy}_{\text{time1}}) * 100$

Algorithm 3:

1) Begin route discovery process

2) If a node receives RREQ packet and if the Energy Consumption rate >thld1 goto 4 else goto 5

3) If a node receives RREP packet then check whether Energy Consumption rate >thld2, If yes goto 4 else goto 5

4) Drop the packet

5) Check the Energy Consumption rate for all nodes in the path and if Energy Consumption rate >thld3, mark that path to indicate high energy consumption or low energy level.

6) stop

RTT module:

RREQ bundle is send from the beginning hub on that time is Rt1 and furthermore set the hour of the RREP parcels. Numerous affirmations are gotten from the goal hub intends to fix the occasions Rt2 I of each RREP bundles. RTT Rt3 I esteems are getting from the Rt1 and Rt2. In view of the Round Trip Time of Rt3 I, process the normal RTT of the considerable number of ways with the assistance of the worth Rts I. After examination of the limit estimation of Round Trip Time Rts I, check whether the aggregate full circle time is not as much as edge full circle time Rtth or not and the bounce tally of specific course is proportional to at least two than the wormhole connect, at that point that course is influenced by wormhole in any case no risk is happened in that wormhole interface. When the wormhole interface is recognized toward that path, at that point sender fixes that hub W1 as wormhole hub and forward bogus RREQ bundle through that specific course I and successor W1 hub. The goal gets bogus RREQ parcel from its successor W2 and recognize that W2 hub as wormhole hub. The hubs W1 and W2 are expelled from the system. At that point consequently wormhole influenced connect is blocked.

Watchdog approach:

Watchdog are perhaps the best instrument to identify the dangers and assaults from the got rowdy and narrow minded hubs in the systems. The Watchdog is utilized to improve throughput in a MANET, by recognizing getting into mischief hubs, which stunt different hubs, by consenting to advance the parcels while never doing as such. While the guard dog is utilized to recognize acting up (malignant) hubs, started by a Replica server, static technique helps directing conventions stay away from these hubs, by expelling them, and making another way. The guard dog happens in each hub in the system.

So as to build the security information exchange, MD5 calculations can be utilized to hash the first passwords and the hash esteems, rather than the plaintext are put away in the database. During confirmation, the info secret word is likewise hashed by MD5 along these lines, and the outcome hash esteem is contrasted and the hash an incentive in the database for that specific client. MD5 forms a variable-length message into a fixed-length yield of 128 bits. MD5 is a well known hash work. It chips away at squares of 512-bits, and procedures each square through 4 rounds, where each round thus forms 16 sub-hinders (each 32-bits). The 512-piece message is separated into 16 sub-obstructs before preparing.

IV.RESULT AND DISCUSSION

SIMULATION PARAMETER:

The simulation parameter is explained as below which is used to produce the simulation suite for proposed solution.

PARAMETER	VALUES
Simulator	NS2.35
Routing Protocol	EE-AOMDV
Number of nodes	20,30
Simulation time	180s
Traffic type	TCP
Packet size	1024 bytes
Packet rate	8packets/sec
Maximum speed	30m/sec

Table 1.1: simulation parameter table

Comparison of our work with existing method:

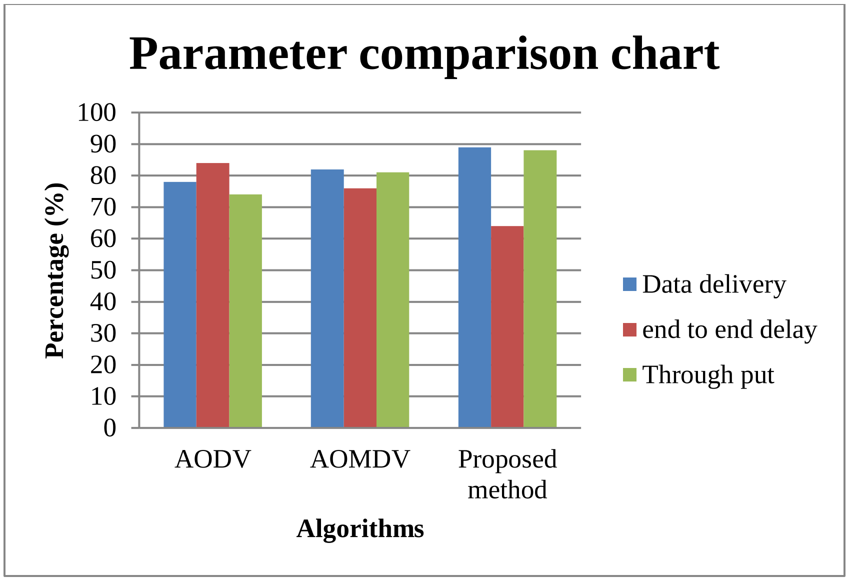

Figure 2: comparison chart

The above graph shows the parameter comparisons such as data delivery, end to end delay, through put. Compared to other existing two methods our proposed work achieves better results.

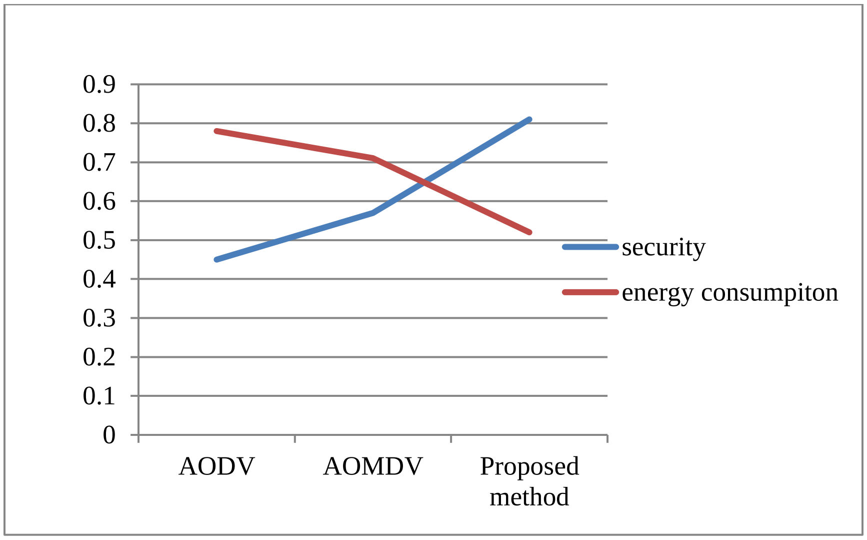

Figure 3: comparison of performance evaluation

Hence the results obtained through our proposed method achieve better results compared to existing methods and it achieves better performance.

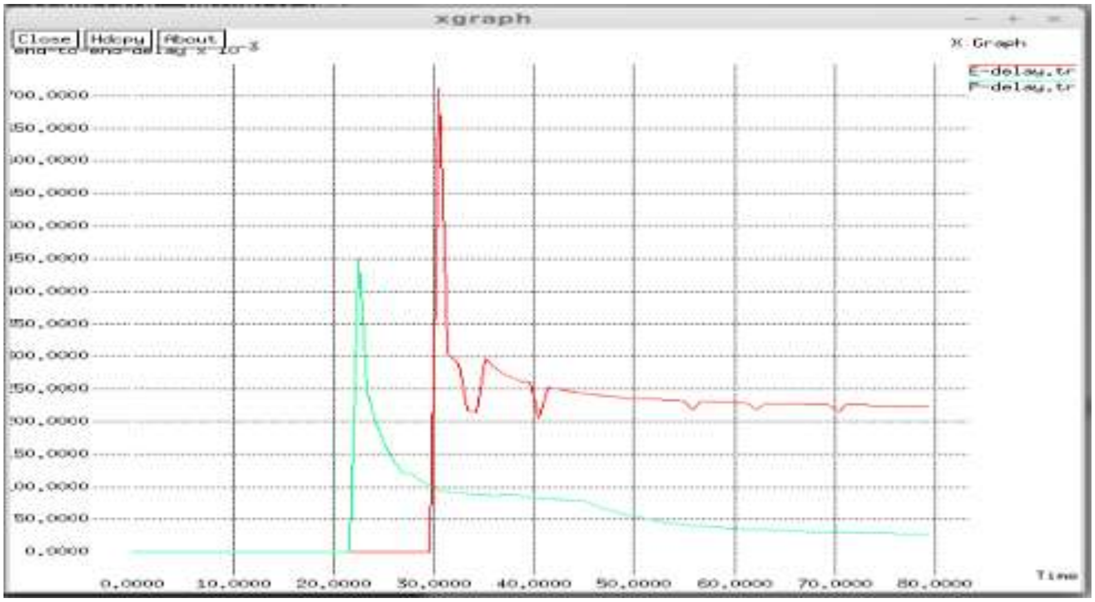

Figure 4: End to end delay

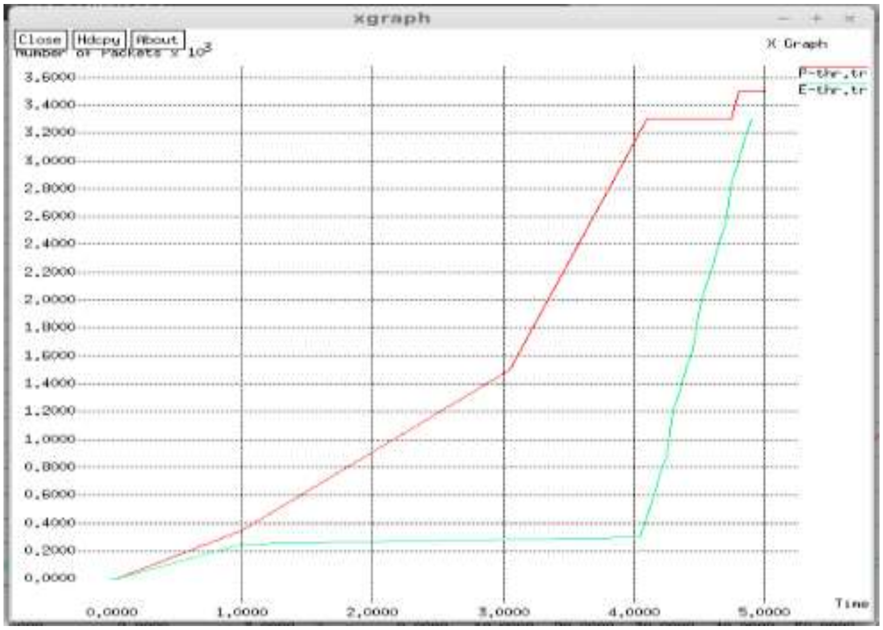

Figure 5: Through put comparison

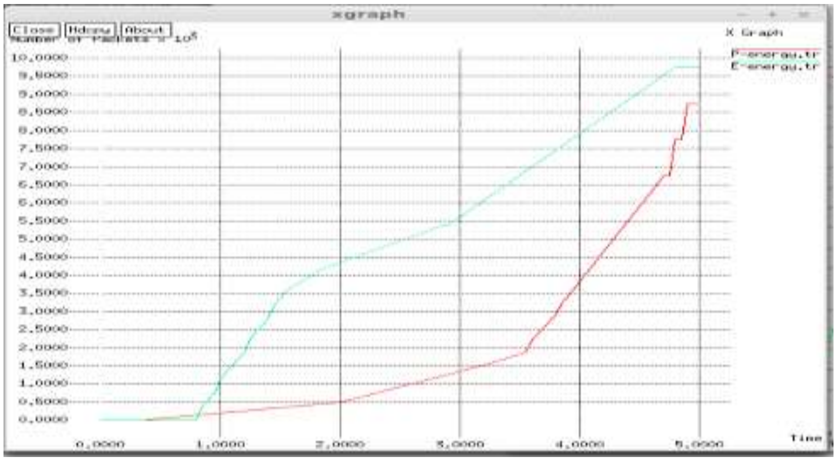

Figure 6: energy consumption

CONCLUSION:

The objective of our work is to increase network lifetime and enable secure data transaction in WSN. This has been achieved in our work through implementing EE-AOMDV which selects best path among various paths and it considered minimum energy and it selects node with high residual energy level. In addition data should be transmitted without any attack and most critical attack as wormhole attack is focused and avoided by hybrid approach of RTT and Watch dog method. In order to protect our data from other forms of attack MD5 encryption is implemented which protect our data from other forms of attack. Hence our proposed method and results shows our methods achieves better result compared to existing methods.

REFERENCES

[1] Muhammad Imran, Farrukh Aslam Khan, Tauseef Jamal, Muhammad Hanif Durad, “Analysis of Detection Features for Wormhole Attacks in MANETs” International Workshop on Cyber Security and Digital Investigation (CSDI 2015).

[2] Ajay Prakash Rai, Vineet Srivastava, Rinkoo B, “Wormhole Attack Detection in Mobile Ad Hoc Networks” International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012.

[3] Louazani Ahmed, Sekhri Larbi, Kechar Bouabdellah, “A Security Scheme against Wormhole Attack in MAC Layer for Delay Sensitive Wireless Sensor Networks” I.J. Information Technology and Computer Science, 2014, 12, 1-10.

[4] Soorya V Nair and Shijin Knox G U, “Energy Efficiency and Network Lifetime Improvement in MANET using AOMDV” International Journal of Engineering Research &amp; Technology (IJERT) Vol. 8 Issue 08, August-2019.

[5] Mary Cindy Ah Kioon, ZhaoShun Wang and Shubra Deb Das, “Security Analysis of MD5 algorithm in Password Storage” Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation (ISCCCA-13).

[6] Mrs. C. Gayathri and Dr.R. Vadivel, “Survey Of Watchdog Mechanism Used For Malicious Node Detection” International Journal of Advanced Research in Computer Science Volume 8, No. 9, November-December 2017.

[7] A. S. K. Pathan, H.-W. Lee, and C. S. Hong, ``Security in wireless sensor networks: Issues and challenges,&#39;&#39; in Proc. 8th Int. Conf. Adv. Commun. Technol., Feb. 2006, p. 6.

[8] G. Farjamnia, Y. Gasimov, and C. Kazimov, ``Review of the techniques against the wormhole attacks on wireless sensor networks,&#39;&#39; Wireless Pers. Commun., vol. 105, no. 4, pp. 15611584, Apr. 2019.

[9] Y.-C. Hu, A. Perrig, and D. B. Johnson, ``Wormhole attacks in wireless networks,&#39;&#39; IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 370380, Feb. 2006.

[10] L. Ahmed, S. Larbi, and K. Bouabdellah, ``A security scheme against wormhole attack in MAC layer for delay sensitive wireless sensor networks,&#39;&#39; Int. J. Inf. Technol. Comput. Sci., vol. 12, pp. 110, Nov. 2014.