International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

LOWER ACTIVITY ADAPTIVE ABSORPTION HIERARCHY CONVENTION POWER UTILIZATION USING LEACH PROTOCOL IN WSN

Dr.C.Nalini[1], G. Lakshmi Vara Prasad[2]

[1]Professor, Department of CSE, Bharath Institute of Higher Education and Reseach University , Chennai

[2]Research Scholar, Department of CSE, Bharath Institute of Higher Education and Reseach University , Chennai

Abstract

Wireless Sensor Networks accept abundant abeyant to abutment several important wireless applications, together with concurrent disc statement, remedial application, inspection purpose sensor networks, automated applications, aggressive surveillance and home networking applications. But there are two arduous issues (i) advice bandwidth and (ii) activity are actual important to architecture wireless and adaptable systems because these are actual abundant bound in arrangement environment. Therefore it requires able advice and architecture techniques to access bandwidth as able-bodied as activity able protocol. The a lot of able acquisition agreement Lower Activity Adaptive Absorption Hierarchy in wireless sensor networks. Lower Activity Adaptive Absorption Hierarchy uses the abstraction of activating absorption if sensor nodes are deploying about area amount of array appulse on the network. This cardboard describes the arrangement superior that depends on altered characteristics of abstracts manual as a Modification on LEACH protocol. In this paper, explain the allegory of magnitude, phase, appearance delay, accumulation delay, amplitude of broadcasting and activity burning respectively.

Key words: wireless sensor; energy efficient; sensor security; attack

Introduction

As of late, the remote sensor systems have ended up one of the hotly debated issue of region of examination. Remote correspondence has demonstrated its various favorable circumstances over wired correspondence and has inside the most recent decade turn into a consistent method of correspondence in individuals' ordinary lives.The rundown of potential uses for remote sensor systems is by all accounts unending, with various applications regions, for example, security, solution, modern hardware observing, the military, agribusiness and others. These systems are no more restricted to military applications however are utilized as a part of a wide cluster of uses including natural surroundings observing [1], mechanical procedure checking [2], activity control [3], [4], medicinal services [5], and so on. This paper [6] enhances the present security systems in remote sensor systems and decreasing force utilization. Drain convention gives a vitality directing convention. Be that as it may, it doesn't cover the security issues. On the other hand, this paper means to give an enhanced secure and more vitality proficient directing convention said "Lightweight Secure LEACH" affirmation computation is incorporated to guarantee information uprightness, validness and accessibility. Moreover, this paper demonstrates the change over Lower Activity Adaptive Absorption Hierarchy convention that makes it secure and how to make it more vitality productive to diminish the impact of the overhead vitality utilization from the additional efforts to establish safety. In [7] group based directing in remote sensor systems is concentrated decisively. Further, creators alter a standout amongst the most unmistakable remote sensor system's directing convention "Drain" as changed Low-energy adaptive clustering hierarchy -“MODLEACH” by presenting productive bunch head substitution plan and dual transmit control level. Our changed Low-energy adaptive clustering hierarchy, in correlation with Low-energy adaptive clustering hierarchy out performs it utilizing measurements of group head arrangement, through put and system life. A while later, hard and delicate edges are executed on adjusted Low-energy adaptive clustering hierarchy -“MODLEACH” that gloats the execution considerably more. In [8] an enhanced directing calculation taking into account Low-energy adaptive clustering hierarchy, known as ILEACH, is proposed in this paper. Firstly, the ILEACH utilized the leftover vitality to

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

shape bunching, which can stay away from the low vitality hub turning into a group head. Besides, a vitality capacity is proposed to adjust the vitality utilization among bunch heads. At last, an information total tree is built to transmit the information from the group heads to sink hub. Remote sensor systems comprises sensors which impart to sensors by multihop. By and large research is proceeding on sensor system through two phases, toward the starting stage is essentially expected for hub and the last stage is for system level issues. The primary examination works in this stage include the system layer and MAC layer convention in view of vitality enhancement, hub localisation innovation, clock synchronization innovation and information combination innovation [9]. As the force of the sensor hub can't be expanded then how the hubs can be effectively use in the system so that framework vitality turns into the prime variable for outlining steering convention. In this paper, we proposed another vitality model in our convention and contrast a few perspectives and existing Lower Activity Adaptive Absorption Hierarchy convention. In remote sensor systems, there are numerous applications that require a high security level. Case in point, military and medicinal services applications. Such applications require most extreme security. Be that as it may, an expansion in security expends more assets [7]. At the point when more assets are devoured it can contrarily affect the lifespan of the system. Remote sensors ought to have the most extreme security with insignificant force utilization to guarantee secure correspondence [8-10]. In the writing, numerous vitality proficient conventions were proposed. Filter convention-"Low-Energy Adaptive Clustering Hierarchy" [11] appeared in Fig. 1 is a self-sorting out and taking into account bunching progressive system which can be-at the "Minimum Transmission Energy(MTE)" convention by 8 times.

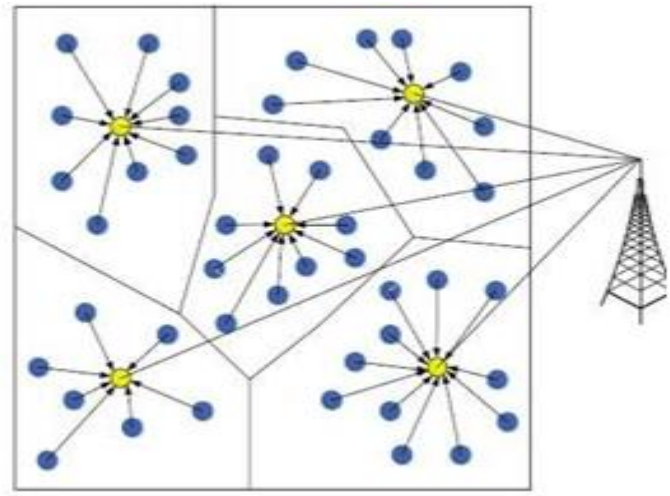

Figure. 1. LEACH Clustering Hierarchy

In this paper, we give efforts to establish safety to Lower Activity Adaptive Absorption Hierarchy convention subsequent to demonstrating the source and confinement of hubs. Likewise, we create efforts to establish safety to shield remote sensors and the interchanges from conceivable assaults without trading off the system execution. Case in point, securing Lower Activity Adaptive Absorption Hierarchy convention against disavowal of administration assaults while keeping up its execution. Besides, the convention guarantees that exclusive the verified hubs are permitted to join and imparted in the system. At the other hand, we alleviate the overhead cost from the efforts to establish safety connected to abstain from trading off the system execution.

Related Work

Safety problems in faraway sensor methods are difficult particularly the world beneath dialogue of set of connections accessibility. Securing faraway sensor methods has been a dynamic exploration box that means to offer solutions for the various more or less attacks which might be known with privateness, respectability and accessibility. In [12], a dynamic association used to be proposed to differentiate DoS attacks. This association embraces Decrease Task Adaptive Absorption Hierarchy conference and comprises some other hub. On this method, there are 3 types of hubs within the gadget which might be detecting, analyzing and team head.

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

Detecting hubs simply plays detecting and the bunch head performs out the necessary conglomeration. Be that as it is going to, the incentive at the back of the brand new type of hubs breaking down hubs or controlling hubs is to inspect the task in each and every staff. As soon as abnormal motion is known, the controlling hubs make a report back to the bunch head. Choosing the controlling hubs will depend on the Multiplicative Linear - Congruential Turbines to haphazardly pick out hubs a few of the hubs with top energy ultimate.For determine Trail DoS the place an aggressor surges the correspondence tactics with replayed or infused bundles to worsen the interchanges medium. The proposed association characterizes unique kinds of hubs which might be an element, aggregator, midway and sink hubs. Phase hubs carry out required detecting. An aggregator hub gathers knowledge from the people and the center of the street hubs are the connections among the aggregator hubs and the sink. After all, the proposed association has the a couple of presumptions which would possibly not now not be affordable. First of all, the moveable hub has no drive barriers and it has a protected correspondence with the bottom station. 2d, phase hubs actualize one-method hash capability while sending knowledge to the aggregator and their pre-dispersed secret is imparted to the center of the street hubs. To spot device attacks, midway hubs make sure the hash esteem ahead of passing bundles and document any atypical practices. A protecting construction towards DoS attacks in far flung sensor methods used to be proposed in [14]. As a way to acknowledge and recoup from a couple of attacks akin to device sticking, flooding and weariness the gadget has important ranges that are the attack popularity and the shield counter estimation. The construction contains of 2 methods; the sensor device and the protect gadget. The sensor device has 4 kinds of hubs that are sensor hubs, protect canine, bunch head and sink. Sensor hubs for info amassing, protect canine sensors for correspondence watching, bunch head for info accumulation and the sink. There are a couple of portions in command of correspondence, attack discovery, protect and consumer keep an eye on. Within the attack region, there are a couple of popularity modules to differentiate numerous types of DoS attacks. After the identity, it asks for the countermeasure phase to make the elemental transfer. In [15] Stavrou and Pitsillides assessed gadget healing after more than a few attacks, retaining in thoughts the top purpose to building up some other conference to make stronger the healing in faraway sensor techniques. The proposed conference has characteristics; acknowledge malevolent motion and separate the tainted hub from gadget. 4 methods of evaluation have been applied; Blacklisting malignant hubs, Cryptographic keys repudiation, Low legal responsibility cycle, and Channel bouncing. The proposed conference can boost up the interruption popularity procedure and fast recovery. In [16], the creators watch the behavior of 2 conventions with specific calculations. First of all conference is Tiny Sec with CBC-MAC calculation. Therefore, stumbling blocks are found out, as an example, the potential of message solution attack and device extend. The second one conference is Tiny ECC with Elliptic Curve Virtual Signature Set of rules. This conference finally ends up being extra unpredictable than the primary conference because it comprises key conveyance and management. On the different hand, coping with time used to be faster in the main conference than the second one. One very important check that analysts extensively tended to is the constraint of energy in faraway sensor methods. In [17], the creators show a solution in gentle of LEACH which they name E-LEACH. E-LEACH complements the lifespan of the device. Whilst referencing the transmission of a large number of knowledge, E-LEACH is simpler then LEACH. As to while the primary hub bites the mud and part hub passes on, E-LEACH signifies higher execution. It adjustments the crowd head after each and every cycle to flow into bunch head energy usage on all hubs. This results in minimizing the energy usage so it may be applied for safety administrations.

Proposed Protocol

The attributes of the keep in touch medium make the faraway sensor methods powerless towards a couple of attacks. An aggressor may just sign up for the device and work out the best way to seize, pay attention in, infuse or transmit knowledge. To remove darkness from the majority of the attacks, we want to successfully play out more than a few undertakings. To begin with, deflect the aggressors from becoming a member of the gadget using gentle weight and energy efficient validation capability the place the bunch head confirms the genuineness of hubs requesting to sign up for the teams in a energy effective method. 2d, represent a restrict for the atypical hub to hub selection of institutions amid time t. Therefore, each and every some of the hubs within the device want to monitor the volume of occasions any hub presented an affiliation with the evaluating hub. This facet is

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

be applied to spot any abnormal successfully from a hub making an attempt to cut price exchange hubs. 3rd, seeing that Decrease Task Adaptive Absorption Hierarchy makes use of an altered TDMA plan each and every hub can simply ship knowledge to the bunch head amid that point. Some other timetable must be applied for each and every hub figuring out while the hub is out there to get knowledge from the crowd head.

A. Node Authentication: In the beginning, we settle for that each and every hub is equipped with thriller keys. One key imparted to the bottom station and any other key shared among all hubs. The personal key imparted to the bottom station is applied while the hub becomes a gaggle head. However, the collection key's applied to sign up for teams. To prevent the assailant from getting access to the gadget, validation should be performed on each the crowd head while it chooses itself and the hubs while they want to sign up for the device. Hubs test the validness of the hub making certain to be the crowd head prior to they ship their becoming a member of call for. As soon as the hubs test the bunch head validness, they may be able to merely in advance and make a joint solicitation. The realness of the hubs soliciting for to sign up for the bunch is checked through the crowd head prior to they develop into a person from that bunch. Determination for the next spherical bunch heads is completed sooner than the top of the present spherical and the wining hub is demonstrated by way of present workforce head to the bottom station a little while later. In consequence, hubs are recommended via the bottom station and the existing workforce head concerning the bunch units out selected towards the next spherical.

B. Finding Unusual motion within the gadget: For additional safety and within the adventure that an aggressor found out how to sign up for the device, we need to actualize a popularity process within the bunches. Taking into account the usage of Decrease Task Adaptive Absorption Hierarchy conference, the correspondence occurs among the bunch head and the hubs and the opposite direction round. Each and every hub assists in keeping up a log to retailer the affiliation endeavors from other hubs and an aspect should be characterised for the volume of imaginable institutions with the hub from any hub amid time t. On the aspect while the affiliation endeavors succeed in the threshold, the hub should document the ones endeavors to the crowd head. Via the identity process, the assailant is known prior to expending the hub's energy to care for a strategic distance from the aggressor all the time introducing affiliation with the target hub.

C. Sending and Receiving TDMA: Each and every hub within the staff has a specific time the place it will possibly transmit the tips to the bunch head as in LEACH conference. On the other hand some other altered calendar must be available among the hub and the crowd head characterizing the time while the bunch head speaks with the hub. The hub starts to pay attention at specific occasions at the off probability that the bunch head has bundles to be despatched to the bearing on hub [18].

D. Deploying and Becoming a member of Clusters: On this space we temporarily read about the obliged ventures to border the device. Those method are necessary to arrange the sensors sooner than the group and the specified process after the sending to make a choice, sign up for and impart among the bottom station, hubs and the bunch heads.

Step one: All hubs are equipped with keys. The primary key can be imparted to the bottom station and the second one can be shared will all hubs for the underlying level to be applied for bunch becoming a member of procedure.

Step two: The crowd heads are selected and make the most of their personal key to talk with the bottom station.

Step three: Nodes make the most of their collecting key to call for becoming a member of the proposed bunch as gave the impression in Fig 2.

Step four: After framing the teams, the bunch head can overhaul the crowd key giving an alternative key than the underlying ones. Likewise, the bottom station can overhaul the crowd head's personal key if required.

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

Step five: Electing a hub for subsequent spherical workforce head should be performed sooner than the top of the present spherical. The existing workforce head tests the legitimacy of the brand new bunch to the bottom station and to the hubs.

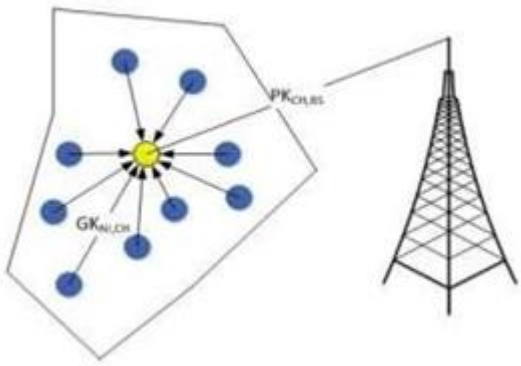

Fig2: Secret and Set input in one cluster

Lightweight Secure Leach for WSN:

On this conference we think that the crowd heads are five% from the mixture choice of the device hubs. The bunch heads can be selected after the device sending and towards the beginning of each and every cycle a at the same time as later. The race of latest bunch heads is from the hubs with probably the most increased residual energy. At that time the existing team head educates the bottom station concerning the legitimacy of the selected bunch head. The message from the bunch head to the primarily based station is scrambled through MAC calculation with the mutual key among the bottom station and the crowd head. After that, the bottom station communicates the rundown of the showed workforce heads to all hubs using uTESLA [19]

$$B.S. \leftarrow {}_{current}CH[MAC[K_{N\text{-}BS}, M]] \quad M={}_{new}CH$$

$$N_i \leftarrow B.S.[\,MAC[K_{N\text{-}BS}, M, [K_{N\text{-}N}]]] \quad M={}_{new}CH_i$$

Next to broadcasting the rundown of the showed bunch heads, hubs can get started a joint solicitation to one of the most team heads. The number of bunch head should be based at the separation among the crowd and the hub to reduce the energy required while talking with each and every different.

A. Election

The race for the next spherical occurs in advance of time within the present spherical. Hubs are selected as a host heads while they have got extra energy staying than exchange hubs (Ni> energyNi). Moreover they will have to have an excellent signal with base station (Ni> signalNi).

while [current round ≠ end]
if $N_i >{}_{energy}N_i$ and B.S $\leftarrow N_i >{}_{signal}N_i$
then ${}_{new}CH \leftarrow N_i$

Within the wake of broadcasting the rundown of the confirmed bunch heads, hubs can get started a joint solicitation to some of the workforce heads. The choice of staff head must be based at the separation among the bunch and the hub to reduce the energy required while talking with each and every different.

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

B. Connection

After the race of the brand new bunch head and informing the bottom station, the bottom station keep up a correspondence to all hubs the rundown of the brand new teams head using uTESLA. Likewise it transmits the average watchword to be applied to sign up for the brand new staff heads ([KN-BS, M, [KN-N]]).

```
do
  if new CH = CH
      then B.S. ← current CH[MAC[K N-BS, M]]          4 bytes
          Ni ← B.S.[ MAC[K N-BS, M, [K N-N]]]         4 bytes
while [current round ≠ end]
```

Toward the start of another surrounding, the bunch head sends a confirmation message (check [M]) with key (KN-N) to neighbor's hubs. In the wake of accepting the message, hubs answer to the bunch head's solicitation by a confirmation message encoded by the common key ([KN-N, validation [M]]) asking for to join the group. In any case, the bunch make a beeline for ensure that it doesn't permit the quantity of hubs to surpass the permitted number in group (Ni<_ 20 Ni). Then again, hubs must demand to join the bunches nearer to them to diminish the vitality utilization in getting and transmitting (new CH > flag new CH).

C. Transmission

The system hubs have three stases; detecting, tuning in/transmitting and resting. Detecting happens when the hubs are detecting the earth. Tuning in/Transmitting happens when hubs are hoping to have correspondence with the group head or base station. Dozing happens when the hubs are hub in detecting or tuning in/Transmitting modes. This requires the hubs to be in rest mode to stay away from the catching which expend hubs vitality. Hubs are required to have a log for the associations endeavors that are initialed with them. At the point when the endeavors come to a predefined limit, a banner is raised to the group head and the base station. The base station needs to play out the fundamental activities on the off chance that the sensor is under assault.

```
while [current round ≠ end]
    then while Ni = sleep or CH = sleep
          if(CH ← new CH[MAC[K N-N, [M]]
            CH ← report
          if(CH ← Ni[MAC[K N-N, M]])
            B.S ← report
```

System existence moment:

Under determine demonstrates the framework throughput contrasting among the based LEACH conference, and the proposed Lightweight secure LEACH. The proposed conference has higher execution because it attempts to average the very best listening by way of striking the hubs in resting state which cut down the pressure usage allowing the hubs to are living extra and to reduce the affects. The standard Leach conference give up acting due to the fact each and every one of the crucial hubs handed on at time 360 that is after 19 rounds. After all, the proposed conference persisted acting till time 475 that is after 24 rounds. Beneath determine demonstrates the correlation among the standard LEACH conference and the proposed conference so far as device lifestyles time. At time 210 sec, conventional LEACH conference started to lose hubs, and via time 368, so much hubs arise brief on drive (while CH < five). On the other hand, Decrease Task Adaptive Absorption Hierarchy with safety misplaced the primary hub at time 360 and misplaced the majority of the hubs (while CH<five) at time 471. Taking a look on the energy usage among strange LEACH and clear out with safety within the beneath determine we find the proposed conference has much less energy usage. As a consequence, peculiar LEACH stored going till time 364 and the proposed conference persisted till time 371. The growth of pressure usage in LEACH conference started at time 210 with the lack of the fundamental hub. Therefore, exchange hubs faced extra load as a result of the growth of pressure usage which lessened the device lifestyles. On the other hand, the

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

proposed conference misplaced the primary hub at time 360. This faded the drive usage and increased the device lifestyles time.

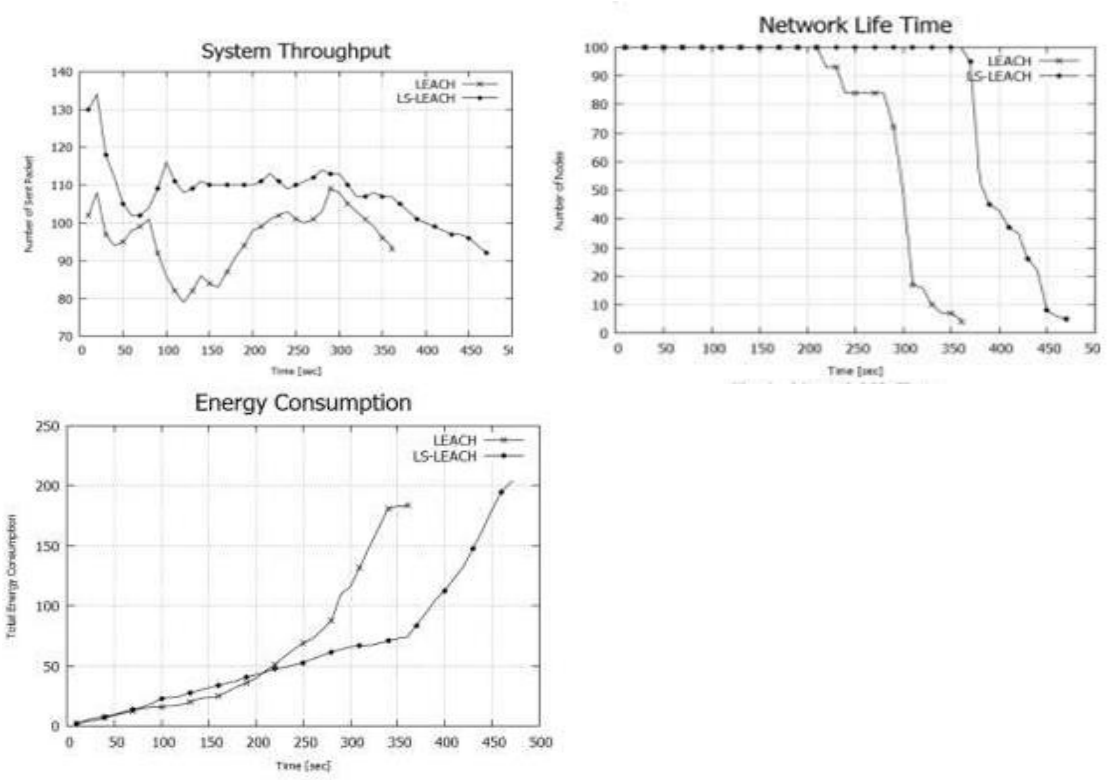

Fig 3: Mock-up results graphs

Conclusion

In this paper we have presented and actualized Lightweight Secure LEACH which is a change of Lower Activity Adaptive Absorption Hierarchy convention. In the wake of enhancing Lower Activity Adaptive Absorption Hierarchy convention power utilization and including the efforts to establish safety, the convention performed better regarding the framework throughput, system existence moment and the aggregate vitality utilization. The planned convention gave a safe validation convention to the system where the new hubs asking for to join the system must be verified with a specific end goal to join the system.

References

1. M. V. Ramesh, A. B. Raj, and T. Hemalatha, "Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks," in Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on, Mathura, 2012, pp. 783-787.

2. L. Gheorghe, R. Rughinis, R. Deaconescu, and N. Tapus, "Authentication and Anti-replay Security Protocol for Wireless Sensor Networks," in Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on, Nice, France, 2010, pp. 7-13.M. Rahman, S. Sampalli, and S. Hussain, "A robust pair-wise and group key management protocol for wireless sensor network," in GLOBECOM Workshops (GC Wkshps), 2010 IEEE, Miami, FL, 2010, pp. 1528-1532.

3. M. El-Saadawy and E. Shaaban, "Enhancing S- LEACH security for wireless sensor networks," in Electro/Information Technology (EIT), 2012 IEEE International Conference on, 2012, pp. 1-6.

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

4. H. Soroush, M. Salajegheh, and T. Dimitriou, "Providing transparent security services to sensor networks," in Communications, 2007. ICC'07. IEEE International Conference on, Glasgow, 2007, pp. 3431-3436.

5. D. Martynov, J. Roman, S. Vaidya, and H. Fu, "Design and implementation of an intrusion detection system for wireless sensor networks," in Electro/Information Technology, 2007 IEEE International Conference on, Chicago, IL, 2007, pp. 507-512.

6. L. Sang Hyuk, L. Soobin, S. Heecheol, and L. Hwang-Soo, "Wireless sensor network design for tactical military applications : Remote large-scale environments," in Military Communications Conference, 2009. MILCOM 2009. IEEE, 2009, pp. 1-7.

7. H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks," in Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on, 2011, pp. 308-311.

8. D. E. Burgner and L. A. Wahsheh, "Security of Wireless Sensor Networks," in Information Technology: New Generations (ITNG), 2011 Eighth International Conference on, 2011, pp. 315- 320.

9. A. Blilat, A. Bouayad, N. El Houda Chaoui, and M. E. Ghazi, "Wireless sensor network: Security challenges," in Network Security and Systems (JNS2), 2012 National Days of, 2012, pp. 68-72.

10. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in International Conference on System Sciences, Maui, Hawaii, 2000, pp. 1-10.

11. M. Guechari, L. Mokdad, and S. Tan, "Dynamic solution for detecting denial of service attacks in wireless sensor networks," in IEEE ICC Ad-hoc and Sensor Networking Symposium, Ottawa, ON, Canada, 2012, pp. 173-177.

12. L. Bai and L. Batten, "Using Mobile Agents to Detect Node Compromise in Path-Based DoS Attacks on Wireless Sensor Networks," in Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007.

13. L. Bai and L. Batten, "Using Mobile Agents to Detect Node Compromise in Path-Based DoS Attacks on Wireless Sensor Networks," in Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on, Shanghai, China, 2007, pp. 2507-2510.

14. Y. Xin, B. Tian, Q. Li, J.-y. Zhang, Z.-M. Hu, and Y. Xin, "A Novel Framework of Defense System Against DoS Attacks in Wireless Sensor Networks," in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, Wuhan, 2011, pp. 1-5.

15. E. Stavrou and A. Pitsillides, "Vulnerability assessment of intrusion recovery countermeasures in wireless sensor networks," in Computers and Communications (ISCC), 2011 IEEE Symposium on, Kerkyra, 2011, pp. 706-712.

16. V. Cionca, T. Newe, and V. Dadarlat, "On the (im) possibility of denial of service attacks exploiting authentication overhead in WSNs," in Sensors Applications Symposium, 2009. SAS 2009. IEEE, 2009, pp. 74-79.

17. J. Xu, N. Jin, X. Lou, T. Peng, Q. Zhou, and Y. Chen, "Improvement of LEACH protocol for WSN," in Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on, 2012, pp. 2174-2177.

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

18. Y. Wei, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," IEEE/ACM Transactions on Networking, vol. 12, pp. 493-506, 2004.

19. A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and E. Culler, "SPINS: Security protocols for sensor networks," Wireless networks, vol. 8, pp. 521-534, 2002.

20. L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, and A. A. Loureiro, "SecLEACH-A random key distribution solution for securing clustered sensor networks," in Network Computing and Applications, 2006. NCA 2006. Fifth IEEE International Symposium on, 2006, pp. 145-154.

21. L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, and A. A. Loureiro, "SecLEACH-A random key distribution solution for securing clustered sensor networks," in Network Computing and Applications, 2006. NCA 2006. Fifth IEEE International Symposium on, 2006, pp. 145-154.