Asian Journal of Science and Applied Technology
ISSN: 2249-0698 Vol. 6 No. 1, 2017, pp.32-37
© The Research Publication, www.trp.org.in

Design and Development of Finical Frame on Reaction performance Expert Routing Protocol in Sloppy WSN

S. Ravichandran[1], R. Benjohnson[2] and S. Lakshminarayanan[3]
[1]Research Scholar in Department of Computer Science,
Bharathiar University, Coimbatore, Tamil Nadu, India
[2]Assistant Professor in Department of Computer Applications,
Coimbatore Institute of Management and Technology, Coimbatore, Tamil Nadu, India
[3]Assistant Professor in Department of Computer Science & Engineering,
Madha Institute of Engineering and Technology, Chennai, Tamil Nadu, India
Email: ravi17raja@gmail.com & karpagaravi15@gmail.com
benjohnsonr@gmail.com, l_naryn2005@yahoo.co.in
balajihoney@gmail.com

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 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 ampules 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, we discussed and explain the allegory of magnitude, phase, appearance delay, accumulation delay, amplitude of broadcasting and activity burning respectively.**

***Keywords*: wireless sensor; energy efficient; sensor security; attack.**

I. 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, mechanical procedure checking, activity control medicinal services, and so on. This paper 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 called LS-"LEACH-Lightweight Secure LEACH". Confirmation calculation is incorporated to guarantee information uprightness, validness and accessibility. Moreover, this paper demonstrates the changeover 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 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 LEACH-"MODLEACH" by presenting productive bunch head substitution plan and double transmitting power levels. Our changed LEACH, in correlation with LEACH 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 LEACH-"MODLEACH" that gloats the execution considerably more. In [8] an enhanced directing calculation taking into account LEACH, known as ILEACH, is proposed in this paper. Firstly, the ILEACH utilized the leftover vitality to 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.

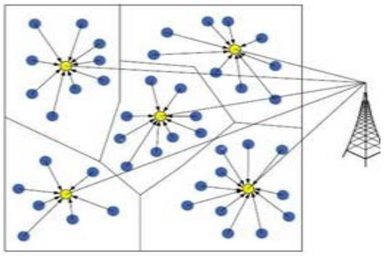


Fig.1 LEACH Clustering Hierarchy

Remote sensor systems comprise 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 localization innovation, clock synchronization innovation and information combination innovation. 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. Such applications require most extreme security. Be that as it may, an expansion in security expends more assets. 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. In the writing, numerous vitality proficient conventions were proposed. Filter convention-“Low-Energy Adaptive Clustering Hierarchy” appeared in Fig. 1 is a self-sorting out and taking into account bunching progressive system which can be-at the MTE (Minimum Transmission Energy) convention by 8 times.

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.

II. RELATED WORK

Security issues in remote sensor systems are challenging especially the area under discussion of set of connections accessibility. Securing remote sensor systems has been a dynamic exploration field meaning to give answers for the diverse kind of assaults that are identified with privacy, respectability and accessibility. In, a dynamic arrangement was proposed to distinguish DoS assaults. This arrangement embraces Lower Activity Adaptive Absorption Hierarchy convention and includes another hub. In this way, there are three sorts of hubs in the systems which are detecting, examining and group head. Detecting hubs just performs detecting and the bunch head plays out the important conglomeration. Be that as it may, the motivation behind the new sort of hubs breaking down hubs or controlling hubs is to examine the activity in every group. Once irregular movement is identified, the controlling hubs make a report to the bunch head. Picking the controlling hubs depends on the Multiplicative Linear - Congenital Generators to haphazardly pick hubs among the hubs with high vitality remaining. For identify Path DoS where an aggressor surges the correspondence ways with replayed or infused bundles to aggravate the interchanges medium. The proposed arrangement characterizes distinctive sorts of hubs which are a part, aggregator, halfway and sink hubs. Part hubs perform required detecting. An aggregator hub gathers information from the individuals and the middle of the road hubs are the connections between the aggregator hubs and the sink. In any case, the proposed arrangement has the a few presumptions. Initially, the portable hub has no force limitations and it has a safe correspondence with the base station. Second, part hubs actualize one-way hash capacity when sending information to the aggregator and their pre-dispersed key is imparted to the middle of the road hubs. To identify system assaults, halfway hubs confirm the hash esteem before passing bundles and report any strange practices. A protective structure against DoS assaults in remote sensor systems was proposed in. So as to recognize and recoup from a few assaults such as system sticking, flooding and weariness the system has two vital stages which are the assault recognition and the guard counter estimation. The structure comprises of two systems; the sensor system and the guard system. The sensor system has four sorts of hubs which are sensor hubs, guard dog, bunch head and sink. Sensor hubs for information gathering guard dog sensors for correspondence observing, bunch head for information accumulation and the sink. There are a few parts in charge of correspondence, assault discovery, and safeguard and client control. In the assault location, there are a few recognition modules to distinguish diverse sorts of DoS assaults. After the identification, it asks for the countermeasure segment to make the fundamental move. In Stavrou and Pitsillides assessed system recuperation after various assaults, keeping in mind the end goal to build up another convention to enhance the recuperation in remote sensor systems. The proposed convention has two qualities; recognize malevolent movement and separate the contaminated hub from system. Four strategies of assessment were utilized; Blacklisting malignant hubs, Cryptographic keys repudiation, Low obligation cycle, and Channel bouncing. The proposed convention can accelerate the interruption recognition process and quick recuperation. In, the creators watch the conduct of two conventions with particular calculations. To begin with convention is Tiny Sec with CBC-MAC calculation. Subsequently, hindrances are discovered, for example, the capability of message answer assault and system delay. The second convention is Tiny ECC with Elliptic Curve Digital Signature Algorithm. This convention ends up being more unpredictable than the main convention since it includes key conveyance and administration. At the other hand, handling time was quicker in the primary convention than the second. One critical test that analysts widely tended to is the constraint of vitality in remote sensor systems. In, the creators display an answer in light of LEACH which they call E-LEACH. E-LEACH enhances the lifespan of the system. While referencing the transmission of a lot of information, E-LEACH is more effective then LEACHES. As to when the main hub bites the dust and half hub passes on, E-LEACH indicates better execution. It changes the group head after each cycle to circulate bunch head vitality utilization on all hubs.

III. PROPOSED PROTOCOL

The attributes of that communicate medium make the remote sensor systems powerless against a few assaults. An aggressor could join the system and figure out how to catch, listen in, infuse or transmit information. To illuminate the vast majority of the assaults, we need to effectively play out various undertakings. To start with, deflect the aggressors from joining the system utilizing light weight and vitality effective validation capacity where the bunch head confirms the genuineness of hubs asking for to join the groups in a vitality productive way. Second, characterize a limit for the ordinary hub to hub number of associations amid time t. Hence, every one of the hubs in the system need to track the quantity of times any hub introduced an association with the comparing hub. This edge is be utilized to identify any irregular effectively from a hub attempting to bargain alternate hubs. Third, since Lower Activity Adaptive Absorption Hierarchy uses an altered TDMA plan every hub can just send information to the bunch head amid that time. Another timetable ought to be utilized for every hub determining when the hub is accessible to get information from the group head.

A.Node Authentication

At first, we accept that every hub is outfitted with two mystery keys. One key imparted to the base station and another key shared between all hubs. The private key imparted to the base station is utilized when the hub turns into a group head. Nonetheless, the gathering key is utilized to join groups. To stop the assailant from accessing the system, validation ought to be done on both the group head when it chooses itself and the hubs when they need to join the system. Hubs check the validness of the hub guaranteeing to be the group head before they send their joining demand. Once the hubs check the bunch head validness, they can simply ahead and make a joint solicitation. The realness of the hubs asking for to join the bunch is checked by the group head before they turn into an individual from that bunch. Decision for the following round bunch heads is done before the end of the current round and the wining hub is verified by current group head to the base station a short time later. Consequently, hubs are advised by the base station and the present group head about the bunch sets out chose toward the following round.

B.Detection Abnormal action inside the system

For further security and in the event that an aggressor figured out how to join the system, we have to actualize a recognition procedure inside these bunches. Considering the utilization of Lower Activity Adaptive Absorption Hierarchy convention, the correspondence happens between the bunch head and the hubs and the other way around. Each hub keeps up a log to store the association endeavors from different hubs and an edge ought to be characterized for the quantity of conceivable associations with the hub from any hub amid time t. At the point when the association endeavors achieve the edge, the hub ought to report those endeavors to the group head. By the identification procedure, the assailant is recognized before expending the hub's vitality to maintain a strategic distance from the aggressor always introducing association with the objective hub.

C.*Sending and Receiving TDMA*

Every hub in the group has a particular time where it can transmit the information to the bunch head as in LEACH convention. However another altered calendar ought to be accessible between the hub and the group head characterizing the time when the bunch head speaks with the hub. The hub begins to listen at particular times on the off chance that the bunch head has bundles to be sent to the relating hub.

D.Deploying and Joining Clusters

In this area we quickly examine the obliged ventures to frame the system. These means are important to set up the sensors before the organization and the required procedure after the sending to choose, join and impart between the base station, hubs and the bunch heads.

Step 1: All hubs are outfitted with two keys. The main key will be imparted to the base station and the second will be shared will all hubs for the underlying stage to be utilized for bunch joining process.
Step 2: The group heads are chosen and utilize their private key to speak with the base station.
Step 3: Nodes utilize their gathering key to demand joining the proposed bunch as appeared in Fig 2.
Step 4: After framing the groups, the bunch head can overhaul the group key giving an alternate key than the underlying ones. Likewise, the base station can overhaul the group head's private key if required.
Step 5: Electing a hub for next round group head ought to be done before the end of the current round. The present group head checks the legitimacy of the new bunch to the base station and to the hubs.

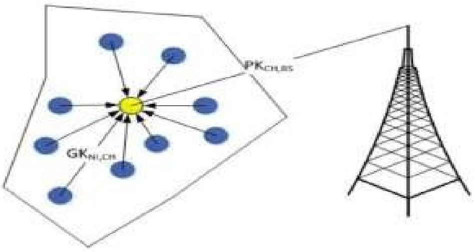


Fig.2 Private and Group Key in one cluster

IV. LS-LEACH FOR WIRELESS SENSOR NETWORKS

In this convention we expect that the group heads are 5% from the aggregate number of the system hubs. The bunch heads will be chosen after the system sending and toward the start of each cycle a while later. The race of new bunch heads is from the hubs with the most elevated residual vitality. At that point the present group head educates the base station about the legitimacy of the chose bunch head. The message from the bunch head to the based station is scrambled by MAC calculation with the mutual key between the base station and the group head. After that, the base station communicates the rundown of the confirmed group heads to all hubs utilizing uTESLA .

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

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

Subsequent to broadcasting the rundown of the confirmed bunch heads, hubs can start a joint solicitation to one of the group heads. The choice of bunch head ought to be founded on the separation between the group and the hub to lessen the vitality required when speaking with each other.

A.Election

The race for the following round happens ahead of time in the current round. Hubs are chosen as a bunch heads when they have more vitality staying than alternate hubs (Ni> energyNi). Furthermore they should have a solid sign with base station (Ni> signalNi).

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

In the wake of broadcasting the rundown of the validated bunch heads, hubs can start a joint solicitation to one of the group heads. The determination of group head ought to be founded on the separation between the bunch and the hub to lessen the vitality required when speaking with each other.

B.Connection

After the race of the new bunch head and informing the base station, the base station communicates to all hubs the rundown of the new groups head utilizing uTESLA. Likewise it transmits the common watchword to be utilized to join the new group heads ([KN-BS, M, [KN-N]]).

```
do
  if $_{new}CH = CH$
      then B.S. $\leftarrow {}_{current}CH[MAC[K_{N\text{-}BS},M]]$          4 bytes
          $N_i \leftarrow$ B.S.[ $MAC[K_{N\text{-}BS},M, [K_{N\text{-}N}]]]$        4 bytes
while [current round $\neq$ end]
```

Toward the start of another round, 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 these 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 stasis; 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 association's 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 $\neq$ end]
    then while $N_i$ = sleep or CH = sleep
            if(CH $\leftarrow {}_{new}CH[MAC[K_{N\text{-}N}, [M]]$
               CH $\leftarrow$ report
            if(CH $\leftarrow N_i[MAC[K_{N\text{-}N}, M]])$
               B.S $\leftarrow$ report
```

V. SIMULATION

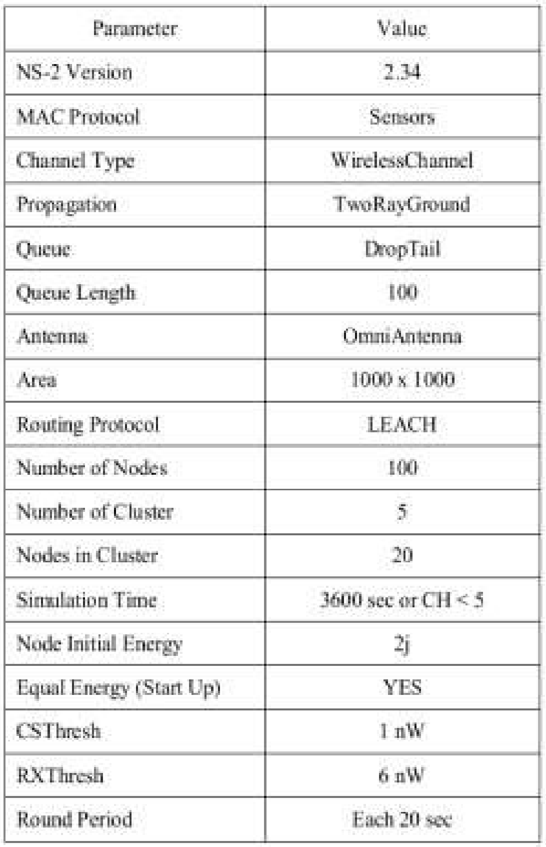
The execution programming of LS-LEACH was conveyed utilizing system test system NS-2. NS-2.34 variant was utilized as a part of this execution and reproduction. NS2 is open source programming under GPL (overall population permit). In addition, NS2 is inherent C++ and the interface is in OTcl dialect which is an item arranged augmentation of TCL dialect. Further, the working framework environment of the recreation was Linux Ubuntu 10.04 LTS introduced on framework with 2.5 GHz Intel Core 2 Duo and 4 GB memory. The usage of LS-LEACH was executed by adding new parameters and capacities to the current

LEACH in NS2. The majority of the progressions were done in the source records of LEACH which are situated in the ns- 2.34 (as in adaptation 2.34) registry in envelope 'mit'. Different changes were likewise done in various documents with the end goal of the connecting of the TCL and C++ as TCL dialect is utilized as the interface for NS2 and OTcl prefers amongst TCL and C++.

A.Simulation Parameters

In simulating LS-LEACH, we have used the following parameters shown in Table 1.

TABLE 1 SIMULATION PARAMETERS



Parameter	Value
NS-2 Version	2.34
MAC Protocol	Sensors
Channel Type	WirelessChannel
Propagation	TwoRayGround
Queue	DropTail
Queue Length	100
Antenna	OmniAntenna
Area	1000 x 1000
Routing Protocol	LEACH
Number of Nodes	100
Number of Cluster	5
Nodes in Cluster	20
Simulation Time	3600 sec or CH < 5
Node Initial Energy	2j
Equal Energy (Start Up)	YES
CSThresh	1 nW
RXThresh	6 nW
Round Period	Each 20 sec

VI. SIMULATION RESULTS

The performance of the system was measured using the system throughput, network life time and the total energy consumption.

A.System Throughput/ Network Life time/

Below figure demonstrates the framework throughput contrasting between the established LEACH convention, and the proposed LS-LEACH. The proposed convention has better execution since it tries to moderate the perfect listening by putting the hubs in resting state which diminish the force utilization permitting the hubs to live more and to lessen the impacts. The typical Leach convention quit performing since every one of the hubs passed on at time 360 which is after 19 rounds. In any case, the proposed convention continued performing until time 475 which is after 24 rounds. Underneath figure demonstrates the correlation between the typical LEACH convention and the proposed convention as far as system life time. At time 210 sec, typical LEACH convention began to lose hubs, and by time 368, most hubs come up short on force (when CH < 5). Then again, Lower Activity Adaptive Absorption Hierarchy with security lost the main hub at time 360 and lost the vast majority of the hubs (when CH<5) at time 471. Looking at the vitality utilization between ordinary LEACH and filter with security in the underneath figure we discover the proposed convention has less power utilization. Accordingly, ordinary LEACH kept going until time 364 and the proposed convention endured until time 371. The expansion of force utilization in LEACH convention began at time 210 with the loss of the principal hub. Subsequently, alternate hubs confronted more load because of the expansion of force utilization which lessened the system life. Then again, the proposed convention lost the main hub at time 360. This diminished the force utilization and expanded the system life time.

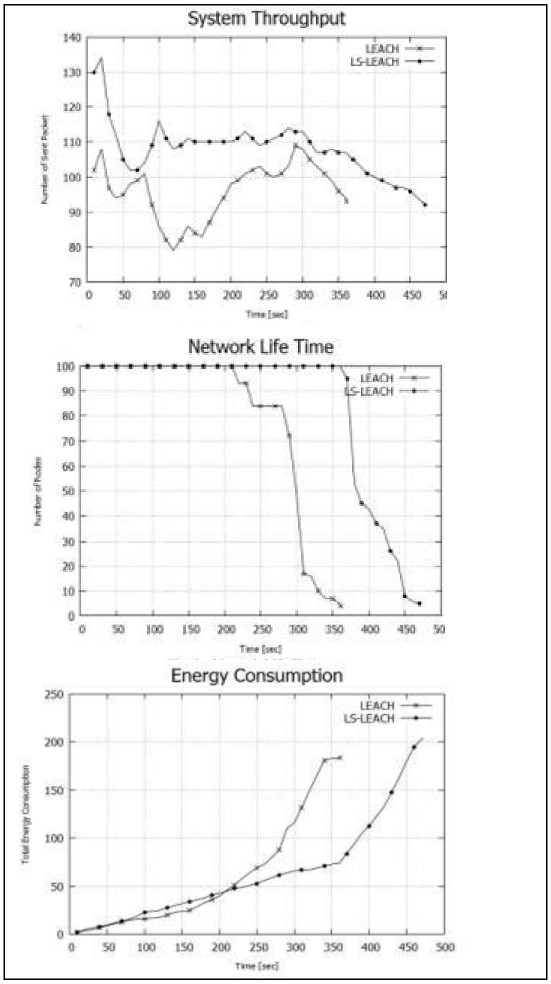


Fig.3 Simulation results graphs

VII. CONCLUSION

In this paper we have presented and actualized LS-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 life time and the aggregate vitality utilization. The proposed 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.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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