ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Authentication Protocol for Clustered Wireless Sensor Networks

Joel Joy Manjaly and J Sandeep
Department of Computer Science
Christ University
Bangalore – 560 029, India

Abstract: Wireless sensor network is an area in wireless computing research which has been receiving a lot of attention recently. This can be mainly attributed to the huge number of potential applications of a wireless sensor network. As wireless sensor networks are primarily employed for sensing tasks, the architecture of the node in the network is fairly simple making them more energy efficient. This is where the main shortcoming of a wireless sensor network is. Due to the simple architecture it is difficult to ensure security in a wireless sensor network, as security protocols need to be lightweight enough to meet the energy constraints of the nodes. This is where this paper comes up with a proposal to enhance an already existing protocol to improve both the security and efficiency of the wireless sensor network.

Keywords: Wireless Sensor Networks; Authentication; Security; Sensor Network Architecture; Clustering

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a type of wireless network with small sensor devices communicating across to exchange crucial information. WSN is the preferred network when requirements for data acquisition from hostile environment arise. But this comes with a huge number of challenges.

In Fig. 1, a typical wireless sensor network has been shown where the source S is sending data to the destination D and from there to the base station. In this example scenario, packet travels through multiple nodes to reach the destination. In Fig. 2, it can be seen how a node connects to the other nodes within its proximity.

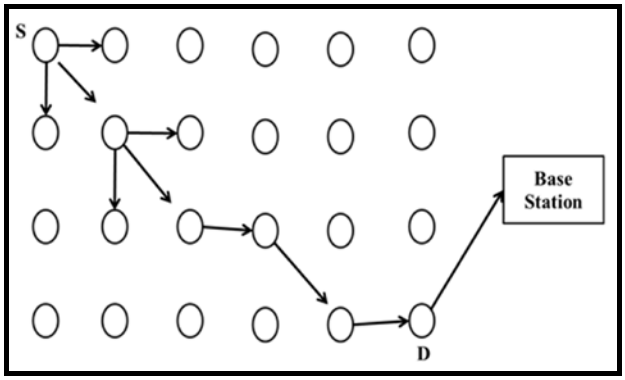

Figure 1. Wireless sensor network.

One of the main challenges in WSNs is security [20]. This is because during the initial period when WSN had just come into existence, their job was to sense from wherever it is deployed to sense and transmit that information to the sink. The sensor device would keep doing this until they ran out of energy and died. This was when adversaries realized that this was something very critical that the developers of WSNs overlooked. The loopholes in WSNs were exploited until WSN developers realized the importance of security. Today this is one of the most popular areas of interest for researchers. An adversary can take over a network in different ways they could deploy sensors of their own in the network, they could capture a node and make it transmit incorrect values, they could make their nodes keep transmitting packets through the network increasing the traffic and thereby reducing the efficiency of the network and so on. In most of the attacks what is seen is a lack of authentication due to which the malicious nodes are able to either transmit or receive intelligible information from the network. Hence the first step in increasing the security of a WSN would be authentication.

Authentication of a node is basically checking of the identity claimed by the node is true or not. The challenge over here is not in creating an authentication protocol, but in creating a protocol which can be used in a WSN without having a huge impact on the performance of the network. There are many protocols in existence which are used in used in other networks which offer very high security. But these protocols cannot be used in WSNs because of the requirement that they must be lightweight. If the protocol used is not lightweight, then most of the energy of the node will be used up on authentication rather than in performing the task for which it was deployed. Hence a balance must be found in the amount of energy a node would spend for authentication and that for the task for which it was deployed.

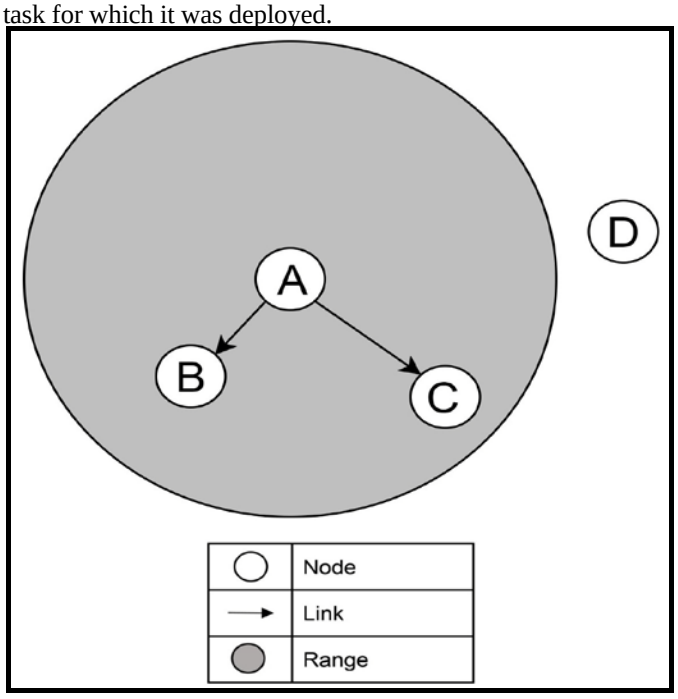

Figure 2. Node connecting with other nodes within its range.

From Network Security basics, authentication can be done in two ways – by using symmetric encryption, or by using asymmetric encryption. In symmetric encryption there would only be one key called the secret key and the messages are encrypted and decrypted using the same key. The disadvantage over here is that an adversary who can get hold of a large number of packets can make an analysis and would be able to eventually crack the key. In asymmetric encryption, we would have two keys – the public key and the private key. When a message is encrypted by one of the two keys it can be decrypted only by the other key. The disadvantage is the requirement of every node in the network to have to store the public keys of all its neighboring nodes. Considering the limitations of both types of encryptions, the one discussed in this paper is a modified form of symmetric encryption which both increases security and at the same time keeps the protocol lightweight enough to be used in a WSN.

II. CHALLENGES AND SECURITY ATTACKS IN WSN

A. *Challenges in WSN*

Some of the main issues and challenges of a WSN are as follows:

1) Energy: The biggest challenge of any WSN is energy or in other words, being energy efficient [22],[23]. There are two reasons for this. One and the most obvious one is because sensor nodes consume energy. There is a need to stress on this point because sensor nodes consume energy for every single task that they perform, from collecting data to processing the collected data to transferring this processed data. Energy is even consumed when the sensor node is idle. This is because it would be listening to communication from the neighbouring nodes. The second reason is because of its limited battery capacity. This is because of the applications of the sensor nodes which need it to be compact in size like for example, deployment in a hostile environment. Once the sensor node's battery runs out of energy there is no possibility of recharging or collecting it back. So it is the duty of the engineers who design it to ensure that sensor node makes the most out of its components, both in terms of performance and in terms in battery life, by using the most efficient hardware architecture as well as software protocols.

2) Self-Management: As WSN is an ad-hoc network, the sensor nodes must be able to cope with the various topologies they may be placed in without human intervention [24],[25]. Once deployed the sensor nodes must be able to independently manage the configuration of the network, recover from the loss of sensor nodes, and guard itself from external adversaries.

3) Calibration: The process of comparing the data obtained from the sensor nodes with some standard values in order to correct them is called calibration [30]. Calibration of data is needed as sensor nodes and the transmitted data themselves could be affected by the environment in which they are located. As manual calibration of sensor nodes is practically impossible due to the sheer number of sensor nodes present in a WSN, we need algorithms which would take care of this. These would become overheads to the actual performance of the WSN [31].

4) Deployment: Another issue with regards to WSN is their deployment. This is a cumbersome activity which only becomes even more so with topology changes [32]. The nodes need to be deployed at fixed locations so that the WSN would be able to operate optimally. In some cases, topologies are inaccessible and hence the sensor nodes would have to be deployed at randomly. Once deployed, the sensor nodes would use clustering algorithms to organize and divide themselves into clusters [33].

5) Freshness: This issue deals with age of the data when it is received by the recipient in other whether the data is past its usefulness [29]. As WSNs are employed for time sensitive tasks, it is important that the data generated by the sensor nodes reach the base station on time for further processing. If there is a delay in the data reaching the base station, due to network congestion or any other factor, the data would, in the worst scenario, end up creating an error during further processing at the base station. Even if the base station is able to detect that this data is old and discard it, the energy which was used by that particular sensor node for detecting and transmitting that data went to waste. Hence it is important to have protocols that help improve the quality of data transmission in the network so as to maintain the required level of freshness of the data.

6) Fault Tolerance: Another issue with WSNs is fault tolerance. Sensor nodes in WSNs stop working or die frequently. During these times, the network must be able to channel the data, that was earlier using the route through the dead node, through a new route. For this purpose, WSNs make use of routing algorithms which although adds on to the overhead of the network, help it in producing more optimal results [34].

7) Security: One another important challenge faced by WSNs is security [26]-[28]. Security is of concern because many of the applications for which WSNs are employed deal with critical data for example, sensing enemy movement in hostile territory, detecting change in sea levels, alarm systems in buildings, etc. In these scenarios any tampering of the data within the WSNs could be catastrophic. The data transferred within the network must be safe from eavesdroppers, as well as adversaries claiming to be a part of the network. This is why there is a need for security in WSN. The challenge with coming up with security protocols for WSNs is that a balance has to be found between allowing the WSNs operate effectively and at the same time securely. This is mainly because the protocols used for security are overheads to the actual requirement for which the WSN was employed. Therefore, their effect on the performance of the WSN must be kept to a minimum. Some of the requirements that security protocols for a WSN must meet are confidentiality, availability, integrity, authentication, freshness and non-repudiation [36].

B. *Security Attacks in WSN*

There are a large number of security attacks against WSNs. They can be broadly classified into two types – passive and active. A passive attack is one in which the adversary merely eavesdrops on the data being transmitted through the network. The intention is to just get hold of confidential information. This kind of attack is hard to detect as there is almost no indication that an adversary has gotten hold of the transmitted data. This type of attack is mostly in preparation for an active attack. In an active attack the adversary will either tamper with the existing data or introduces his own data into the network. Some of the popular security attacks against WSN are as follows.

1) Replayed Routing Information: In this attack, the adversary manipulates the routing information present in the network [36]. This can cause the data sent from one node to another to take a lot longer, packets endlessly replaying through the network and creating unwanted traffic, network partition, etc. This attack takes place in the network layer.

2) Selective Forwarding: In this attack, the malicious or compromised node would forward packets selectively. As a

WSN is a multi-hop network, it is important that every node forwards the packet that it receives to the required destination. This attack is very efficient as it gives the adversary a higher degree of control over the network [20].

3) Node Capture Attack: In this attack, the adversary captures a node and extracts the security information used by it. This could severely affect the security of the entire WSN [20]. One solution to this is to use tamper-resistant nodes, but this would increase the cost of the network. Another solution is to destroy the node, but any misjudgement in determining if a breach had taken place would severely damage the performance of the WSN. No matter which solution is used it does not completely protect the network from this attack as researchers are yet to come up with a protocol that is efficient enough.

4) Sybil Attack: In Sybil attack, the malicious node takes on the identities of several nodes in the WSN at the same time. This would allow the node to disrupt distributed algorithms as it would allow it to take part in elections. Basically it allows the adversary to operate from more than one location at the same time [20].

5) HELLO Flood Attack: In this attack, the malicious node would appear to another node as a nearby node. It would do this by transmitting packets with very transmission power [20]. Hence, the packets would be received at the recipient node without a huge loss in power, and would also request the recipient for a HELLO packet as it appears as its neighbour. The malicious node could keep repeating this for as long as it wants, severely affecting the performance of the recipient node.

6) Jamming: This is an attack in which the adversary would place a jamming source within the proximity of the WSN, thereby interfering the communication between the nodes [20]. Even with jamming sources that are less powerful the adversary can severely affect the performance of the WSN by placing these sources at strategic positions within the network.

7) Wormholes: In this attack, there would be two malicious nodes placed at two ends of the WSN [37]. However, these nodes would appear as neighbouring nodes to the rest of the network. This would cause nodes to send packets through them, which would then be passed between the malicious nodes through a low latency link. This attack affects the performance of the network by unnecessarily increasing the network traffic.

III. RELATED WORK

A. *Literature Survey*

The communication in WSN is done through wireless transmitter-receivers or transceivers and therefore the number of challenges and issues is much higher than other networks. However, it is the routing strategies and network modelling that is getting all the focus these days with very less given to security. In 2006, K. H. Wong et al. proposed a scheme [1] in which the WSN is divided into zones. A user can connect to any of the nodes using his device. But before the user can send a query to the system he has to register using a three phase scheme consisting of registration, login and authentication. The user can send any number of queries to the system during a time period after which the registration must be performed again. This scheme only works against replay and forgery attacks. In 2006, S. Zhu et al. proposed a scheme [2] which has more than one keying mechanisms and it allows establishment of the following kinds of keys – (i) an individual key shared with the base station, (ii) a pair key shared with other WSNs, (iii) a cluster key shared with several neighboring nodes, and (iv) a group key shared by all nodes in the network.

In 2003, Q. Huang et al. proposed a scheme [9]-[11], which made use of Elliptic Curve Cryptography and is successfully able to prevent impersonation attacks. In 2006, S.M. Chang et al. proposed the Lightweight One-Time Signature Scheme [3] in which nodes can authenticate messages coming from the base station. The symmetric cryptographic primitives are used to accomplish the asymmetric property for broadcast authentication. This scheme has four major benefits over similar protocols: no requirement of time synchronization, no buffering needed by a receiver, individual message authentication, and instant message authentication. In 2009, the SPINS protocol [4] was proposed by A. Perrig et al. to offer a common solution to accomplish message authenticity and integrity is to employ a Message Authentication Code (MAC), which is added along with a message as a signature. This protocol seems to be feasible for WSN due to the function of the MAC value.

In 2007, R. Wang et al. proposed a scheme [12] which uses broadcast authentication. This scheme was not successful at preventing malicious node attacks and hence an enhanced scheme [13]-[15] was proposed by P. Ning et al. in 2008 which made use of group key mechanism. In 2011, O. Delgado-Mohatar et al. proposed a scheme [5] which makes use of keyed-hash functions. This scheme also, like previously mentioned schemes, consists of three stages – key distribution, network initialization, and authentication. The key distribution is done when the nodes are manufactured. The key generated and distributed in this scheme is a symmetric one. The second phase takes place when the network is deployed. Upon deployment, each node will discover its neighbours and set up the network. The third phase takes place each time a new node enters the network. It fares well against node capture attack, and also continues to work efficiently when the size of the network increases. In 2010, Y. Qiu et al. proposed a scheme [16] in which every sensor node maintains a table which contains all the pre-shared key pairs in the WSN. This makes the scheme scalable to meet the changing requirements of the WSN. In 2010, T. Zhang et al. proposed scheme [17] for key management which reduces the key storage space required. This scheme is efficient at resisting against node compromising attacks.

In the year 2013, EIBAS [6] was proposed by K.-A. Shim et al. in which the network includes a stationary sink, the users, and the sensor nodes. The sink is assigned the responsibility of generating private keys for all the users of the WSN. The main disadvantage of this scheme is limited storage capacity. The EIBAS scheme addresses two main issues in WSNs – (a) user authentication and message integrity, and (b) reduction in communication overhead. In 2014, LOCHA [7] was proposed by A. R. Chowdhury et al. and had a hashing system which could generate fixed short-length hash digests from user messages. This scheme is lightweight in terms of the communication, computation and storage overheads on the network. In addition, it could also use the generated hash digest in the node and message authentication in the WSN. In 2015, X. Anita et al., X. Fan et al. and M. Singh et al. proposed schemes [8],[18],[19] which used a lot less energy and memory when compared to the other existing routing protocols. Moreover, these protocols also improve the packet delivery ratio of the WSN. In 2015, S. Raja Rajeswari et al. proposed a scheme [21] which uses a symmetric key-based authentication mechanism that gives sleep and wake-up commands to the nodes in the network and thereby improves their energy efficiency. This scheme is said to withstand many of the

common attacks like node capture attack, replay attack, Sybil attack, etc.

B. Problem Definition

Suppose there is a WSN. There is a need to authenticate each node before communicating with them. This is done to ensure that whatever message is received is from a node which belongs to our WSN. Moreover, it also ensures that only nodes belonging to the network can make sense of the data that it receives. S. Raja Rajeswari and V. Seenivasagam in their paper "Secured Energy Conserving Slot-Based Topology Maintenance Protocol for Wireless Sensor Networks", nodes would be given a sleep/wake-up command which would be encrypted using a symmetric key. The sleep/wake-up command is given to improve the energy efficiency of the node. But since symmetric encryption is used and moreover the same secret key is used throughout the duration for which the WSN is used, it is vulnerable to attacks by an analyst who can get hold of the packets transmitted. After getting hold of a large number of packets it would be fairly easy for an analyst to crack the secret key. This would be especially dangerous if the WSN was deployed for some critical task such as a military operation for sensing enemy movement in a region. In this paper, a new authentication protocol is proposed to overcome the above discussed problem.

IV. PROPOSED MODEL

The network architecture of clustered sensor nodes proposed in this paper can be seen in Fig. 3 with its authentication and key distribution hierarchy. In this work the three levels of the network are master, cluster head and member node.

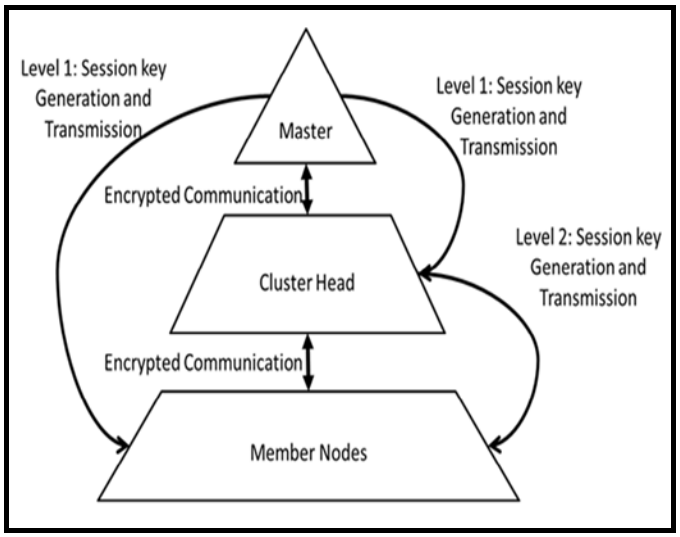

Figure 3. Networking structure with three level authentication.

A. Structure of Network for Authentication Hierarchy

There are two types of networks, structure-less and structured. In a structure-less network, the positions of the nodes are not known before deployment. They can be located anywhere in the network region and in case clustering is required, algorithms can later be applied to group the nodes into inappropriate clusters. In a structured network, each node would be deployed in predetermined locations which would make the clustering process a lot easier but on the other hand the network deployment process would be a little costly. The assumption for this model is that the network would be a structured one rather than a structure-less one.

The various components of the WSN are – sensor nodes, cluster heads and the sink, as can be seen in Fig. 4. The sensor nodes are the individual nodes placed throughout the network whose main task is to gather information and then transmit it, with maybe a small processing involved. In this proposal the sensor nodes are also given the task of encrypting the data it gathered using a session key. The nodes are divided into clusters of manageable sizes with a head called the cluster head. The nodes would only communicate with their cluster heads. The cluster head will then in turn transmit that information to the sink, which is where the information gathered from every node gets collected.

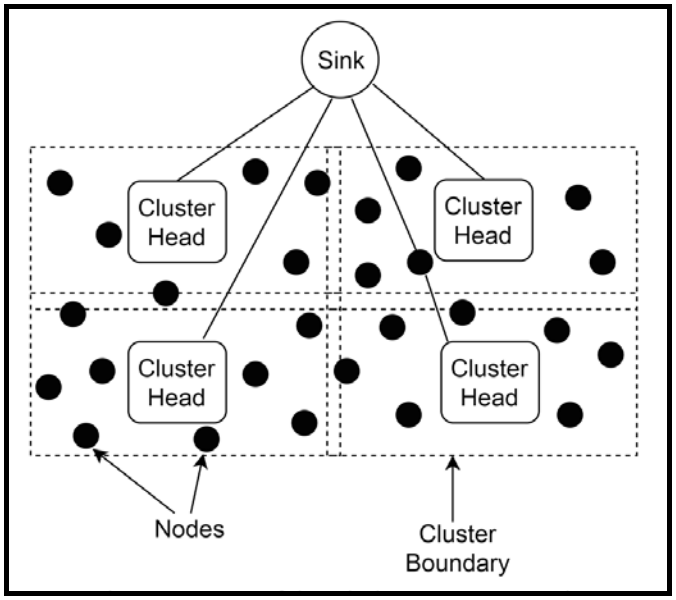

Figure 4. Structure of the wireless sensor network.

1) Sink and Cluster Heads: The communication between the cluster head and the sink is secured using both symmetric as well as asymmetric key encryption. The sink has a public-private key pair of which the public key would be shared with all the cluster heads. Whenever the session key with the cluster heads expire, they would send a request to the sink, encrypted with the Public key of the sink, asking for a new session key. Henceforth, all data transmitted from that particular cluster head to the sink would be encrypted using the new session key. The sink also maintains the master keys of all the cluster heads within its network. The master key is basically a symmetric key which is used by the sink whenever it wants to issue a new session key for a particular cluster head.

2) Cluster Heads and Sensor Nodes: The communication between the cluster head and the sensor nodes in its cluster is secured using asymmetric key encryption alone. The cluster head would have a public-private key pair with it and would share the public key with all the sensor nodes in its cluster. The sensor nodes would encrypt the data transmitted by it to the cluster head using this public key.

B. Authentication Using Session Key

As mentioned earlier, the entire network is divided into clusters with each of them having a node called the cluster head. Each cluster head's secret key will be available with the sink before deployment. After the deployment, the cluster head would have to register with the sink before it can start transmitting data to it. For this, the cluster head sends a request, encrypted using its secret key along with an identifier to the sink. The sink decrypts the request, starts a session and sends the new secret key generated for that session. This packet containing the new secret key would be encrypted using the

previous secret key and sent to the node that had originated the request. Henceforth, whenever any cluster head needs a new session key it follows this procedure to obtain it. The same procedure is followed by each node within a cluster to obtain their secret keys from their respective cluster heads.

Each time before encrypting, the cluster head checks whether the session key it has with it has expired or not, as can be seen in the algorithm flowchart in Fig. 5. It does this by checking the time stamp of the key and comparing it with the allowed time period for a session key. If the key has not expired, it would encrypt it using the same key. Else it would send a request to the sink asking it to generate a new session key for it. It sends this request encrypted using the public key of the sink. The sink would then respond by sending a new session key, along with its time stamp and the time period for which it should be used, which would be encrypted by the master key of that particular cluster head.

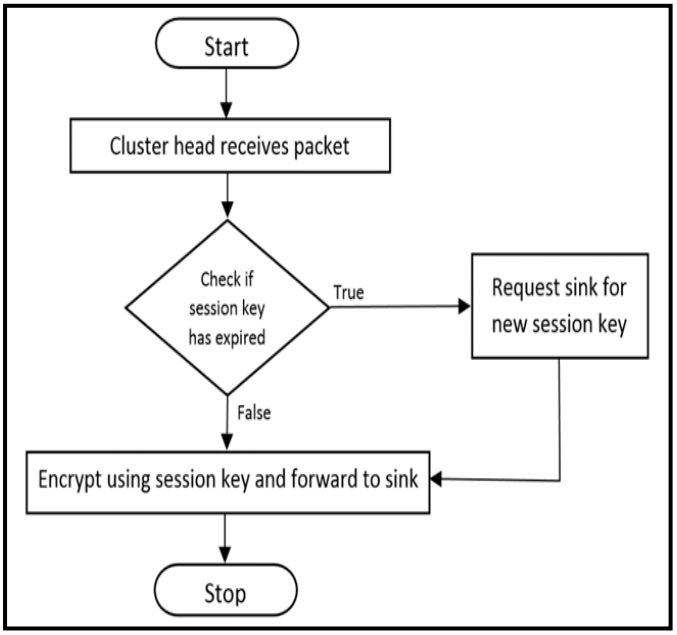

Figure 5. Algorithm to check for expired session key.

C. *Session Key Distribution*

In the previous section the architecture of the network has been discussed. The key distribution in the network is done in a hierarchy, where the upper level node generates the session key for a limited time (session). This session key is then encrypted and forwarded to the lower level members of the node. The model permits any node to request for the session key to its cluster head in response to which the cluster head will authenticate with the registered information of the member node.

D. *Time Stamp*

Every session key that is generated by the sink would also have a time stamp associated with it, which is basically the time at which the session key was generated. This would help in determining when the cluster head needs to send a request to the sink to issue a new session key. Moreover, this would also improve the security of the WSN by reducing the probability of an eavesdropper cracking the key.

$$T = \beta(t) + t \quad (1)$$

The above given equation (1) is used by the cluster head to determine whether the session key that it currently has, has expired or not. In the formula, T is the dynamic time period during which a session key can be used and after which the cluster head has to request the sink to issue a new one. β is a function whose output which would vary from 0 to 1 based on the amount of traffic in the network when the session key was generated. The value of β would tend towards 1 when the network traffic is minimum and to 0 when the network traffic is maximum. Network traffic is taken into account in the calculation of the time period for a session key because there is no need to change the session key immediately if it has hardly been used. t is the constant which has been set when the WSN was deployed.

V. CONCLUSION

Authentication of any node in wireless sensor network is crucial research area in the networking domain. Complexity of the protocol is not supposed to cause higher energy consumption in the network as the devices are limited with its energy. Thereby, wireless sensor network demands for a light weight authentication protocol for higher security in the network. In this paper, an authentication protocol has been proposed for large wireless sensor network. The proposed system has followed the typical architecture with clusters and cluster heads for its internal and external transactions. The proposed system uses session keys for the transaction with the hierarchy in authorization. Future work for the proposed work will include the implementation and analysis of the protocol using simulation tool.

VI. ACKNOWLEDGMENT

The authors would like to thank the Department of Computer Science, Christ University, Bangalore for their kind assistance in this research.

VII. REFERENCES

[1] K. H. Wong, Y. Zheng, J. Cao, and S. Wang, “A dynamic user authentication scheme for wireless sensor networks,” in Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, vol. 1, p. 8, IEEE, Taichung, Taiwan, June 2006.

[2] S. Zhu, S. Setia, and S. Jajodia, “LEAP+: efficient security mechanisms for large-scale distributed sensor networks,” ACM Transactions on Sensor Networks, vol. 2, no. 4, pp. 500–528, 2006.

[3] S.-M. Chang, S. Shieh, W. W. Lin, and C.-M. Hsieh, “An efficient broadcast authentication scheme in wireless sensor networks,” in Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS ’06), pp. 311–320, Taipei, Taiwan, March 2006.

[4] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: security protocols for sensor networks,” Wireless Networks, vol. 8, no. 5, pp. 521–534, 2002.

[5] O. Delgado-Mohatar, A. F´uster-Sabater, and J. M. Sierra, “A light-weight authentication scheme for wireless sensor networks,” Ad Hoc Networks, vol. 9, no. 5, pp. 727–735, 2011.

[6] K.-A. Shim, Y.-R. Lee, and C.-M. Park, “EIBAS: an efficient identity-based broadcast authentication scheme in wireless sensor networks,” Ad Hoc Networks, vol. 11, no. 1, pp. 182–189, 2013.

[7] A. R. Chowdhury, T. Chatterjee, and S. DasBit, “LOCHA: a light-weight one-way cryptographic hash algorithm for wireless sensor network,” Procedia Computer Science, vol. 32, pp. 497–504, 2014.

[8] X. Anita, M. A. Bhagyaveni, and J. M. L. Manickam, “Collaborative lightweight trust management scheme for

wireless sensor networks," Wireless Personal Communications, vol. 80, no. 1, pp. 117–140, 2015.

[9] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," in Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications (WSNA '03), pp. 141–150, San Diego, Calif, USA, September 2003.

[10] P. Vijayakumar and V. Vijayalakshmi, "Effective key establishment and authentication protocol for wireless sensor networks using elliptic curve cryptography," in Proceedings of the Conference on Mobile and Pervasive Computing (CoMPC '08), August 2008.

[11] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," in Proceedings of the 1st Annual IEEE Conference on Communications Society Sensor and Ad Hoc Communications and Networks (SECON '04), Santa Clara, Calif, USA, 2004.

[12] R. Wang, W. Du, and P. Ning, "Containing denial-of-service attacks in broadcast authentication in sensor networks," in Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 71–79, ACM, September 2007.

[13] P. Ning, A. Liu, and W. Du, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks," ACM Transactions on Sensor Networks, vol. 4, article 1, 2008.

[14] Q. Dong, D. Liu, and P. Ning, "Pre-authentication filters: providing dos resistance for signature-based broadcast authentication in sensor networks," in Proceedings of the 1st ACM Conference on Wireless Network Security (WiSec '08), pp. 2–12, ACM, Alexandria, Va, USA, March-April 2008.

[15] X. Sun, X. Wu, C. Huang, Z. Xu, and J. Zhong, "Modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance in wireless sensor networks," Ad Hoc Networks, vol. 37, pp. 324– 336, 2016.

[16] Y. Qiu, J. Zhou, J. Baek, and J. Lopez, "Authentication and key establishment in dynamic wireless sensor networks," Sensors, vol. 10, no. 4, pp. 3718–3731, 2010.

[17] T. Zhang and H. Qu, "A lightweight key management scheme for wireless sensor networks," in Proceedings of the 2nd International Workshop on Education Technology and Computer Science (ETCS '10), pp. 272–275, Wuhan, China, March 2010.

[18] X. Fan and G. Gong, "Lpkm: a lightweight polynomial based key management protocol for distributed wireless sensor networks," in Ad Hoc Networks, vol. 111 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 180–195, Springer, Berlin, Germany, 2013.

[19] M. Singh, A. R. Sardar, R. R. Sahoo, K. Majumder, S. Ray, and S. K. Sarkar, "Lightweight trust model for clustered WSN," in Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, pp. 765–773, Springer, 2015.

[20] S. Raja Rajeswari and V. Seenivasagam, "Comparative Study on Various Authentication Protocols in Wireless Sensor Networks," The Scientific World Journal, vol. 2016, Article ID 6854303, 16 pages, 2016.

[21] S. Raja Rajeswari and V. Seenivasagam, "Secured energy conserving slot-based topology maintenance protocol for wireless sensor networks," Wireless Personal Communications, pp. 1–24, 2015.

[22] M.H. Anisi, A.H. Abdullah, and S.A. Razak, "Energy Efficient Data Collection in Wireless Sensor Networks", Wireless Sensor Networks, vol. 3, 2011, pp. 329-333.

[23] W. Dargie, and C. Poellabauer, Fundamentals of Wireless Sensor Networks: Theory and Practice, Wiley Blackwell, 2010.

[24] K. Sohrabi, J. Gao, V. Ailawadhi and G.J. Pottie, "Protocols for self-organization of a wireless sensor networks", IEEE Personal Communications, vol. 7, no. 5, 2000, pp. 16-27.

[25] S. Vaidyanathan and M. Vaidyanathan, "Wireless Sensor Networks- Issues & Challenges", Information Systems: Behavioral & Social Methods eJournal, 2011, pp. 7.

[26] P. Mohanty, S. Panigrahi, N. Sarma, and S.S. Satapathy, "Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey", Journal of Theoretical and Applied Information Technology, vol. 13, no.1, 2005-2010, pp. 14-27.

[27] M.K. Jain, "Wireless Sensor Networks: Security Issues and Challenges", International Journal of Computer and Information Technology, vol. 2, no. 1, 2011, pp. 62-67.

[28] A.K. Pathan, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. 8th International Conf. Advanced Communication Technology (ICACT'08), vol. 2, 2006, pp. 1043-1048.

[29] J.A. Stankovic, A.D. Wood, and T. He, "Realistic Applications for Wireless Sensor Networks", Theoretical Aspects of Distributed Computing in Sensor Networks, Monographs in Theoretical Computer Science, An EATCS Series, Chapter 25, Springer-Verlag Berlin Heidelberg, 2011, pp. 835-863.

[30] V. Bychkovskiy, S. Megerian, D. Estrin, and M. Potknojak, "A Collaborative Approach to In place Sensor Calibration", Proc. 2nd International Workshop Information Processing in Sensor Networks (IPSN'03), Apr. 2003, pp. 301-316.

[31] J. Feng, S. Megerian and M. Potkonjak, "Model Based Calibration for Sensor Networks", Proc. of IEEE Sensors, vol. 2, Oct. 2003, pp. 737-742.

[32] A. Ahmed, J. Ali, A. Raza and G. Abbas, "Wired Vs Wireless Deployment Support for Wireless Sensor Networks", Proc. IEEE Region 10 Conf. (TENCON 2006), Nov. 2006, pp. 1-3.

[33] J. Li, Y. Bai, H. Ji and D. Qian, "POWER: Planning and Deployment Platform for Wireless Sensor Networks", Proc. 5th International Conf. Grid and Cooperative Computing Workshops (GCCW'06), IEEE, Oct. 2006, pp. 432-436.

[34] M.K. Jain, "Wireless Sensor Networks: Security Issues and Challenges", International Journal of Computer and Information Technology, vol. 2, no. 1, 2011, pp. 62-67.

[35] Rajeev Shorey, Akkihebbal L. Ananda, Mun Choon Chan, and Wei Tsang Ooi, Mobile, Wireless, and Sensor Networks: Technology, Applications, and Future Directions, John Wiley & Sons, Inc, 2006.

[36] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.

[37] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.