International Journal of Grid and Distributed Computing
Vol. 14, No. 1, (2020), pp. 432-441

Conceptual Framework on Assessment of Risk Factor in Wireless Sensor Network

Chavan Sidram Nagnath
Research Scholar, Department of Computer Science,
Dr. A.P.J. Abdul Kalam University, Indore, M.P.

Dr. Deepika Pathak
Research Guide, Department of Computer Science,
Dr. A.P.J. Abdul Kalam University, Indore, M.P.

Abstract

Wireless sensor networks (WSNs) have attracted a lot of interest over the last decade in wireless and mobile computing research community. Applications of WSNs are numerous and growing, which range from indoor deployment scenarios in the home and office to outdoor deployment in adversary's territory in a tactical battleground. We identify the security threats, review proposed security mechanisms for wireless sensor networks. We also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks.

Keywords: WSN, Risk, Sensor, Routing, Coverage**.**

Introduction

A Wireless Sensor Network (WSN) is a community of wireless contact spatially distributed sensor nodes interconnected. As can be shown on Figure 1, an electro-powerful node, also known as a mote, is composed of a processor, a storeroom, the module of the transceiver, a single sensor or several sensors, an ADC converter and a battery power source.

The generations, routing, architecture and WSN storage management have been identified. Additional surveys offer an outline of current sensor network routing protocols. Authors implemented many established sensor network middleware. In many separate ways the writers explored the strategies of sensor localization and the hierarchical taxonomy and the implementations. They launched new method of sensor position and their IoT infrastructure deployment. Authors provided a survey of the device-free position of sensors for the world of information in the same way. In, WSN modeling techniques were surveyed by authors. They presented how the node activity and the network behavior are represented in each procedure. The simulation tool for each strategy was also introduced. However, few works analyzed and addressed the core status of the existing WSN methods for programming and modeling. Motivated by this concept, we present an analysis in which current architecture methodologies of WSN are aggregated and addressed. We research low level, implementation-focused approaches and high-level, model concept-based approaches to the design of WSN systems. The key aim of our research is to analyze the efficacy and implementation of high-level approaches that help to decrease the complexity of WSN systems growth and increase maintenance and portability. High levels of abstraction architecture, focused on the MDE paradigm and in particular on common frameworks such as

ISSN: 2005-4262 IJGDC

the simulation and study of real time and embedded systems (MARTE), profile and design trends have attracted significant interest at present. The WSN method at higher degree of abstraction decreases processes sophistication and improves models' reusability and stability. It also offers automation and increases the consistency of the model. It also includes the early design framework, enabling failures to be identified in anticipation of actual network implementation.

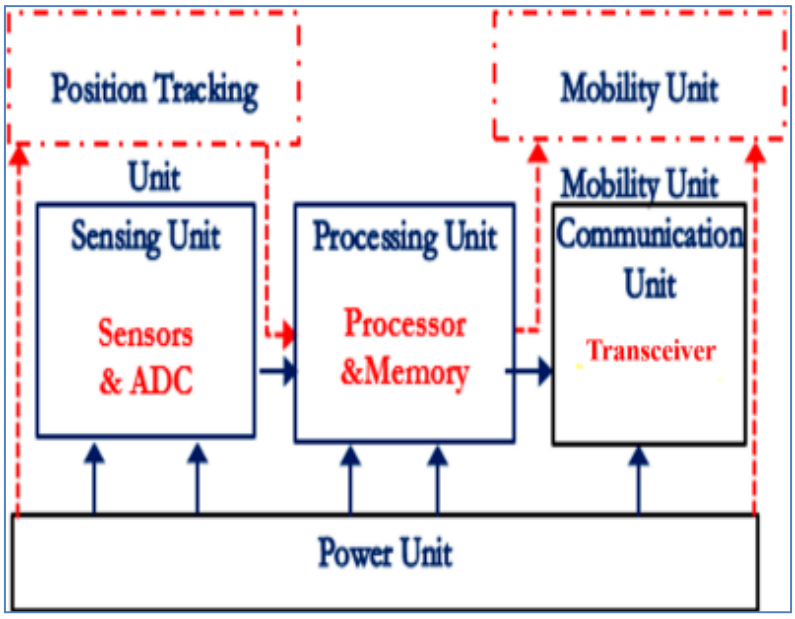

Figure 1. The Typical Architecture of a Sensor Node Used in Wireless Sensor Networks (WSNs)

WSN sensors have a range of roles, capacities and uses. The sector is now evolving under the pull of recent technical advancements and a number of future applications. Early-deployment sensor networks are all examples of radar networks used for monitoring of aviation, national energy supplies and national weather stations deployees over a normal topographic map, all of which require sophisticated machines and protocols of communication and are therefore quite costly.

Image. 2 demonstrates an instance of sensor network data flows. In some instances, there are no energetic or communications infrastructures in the area to be tracked and it is important that sensor nodes safeguard themselves from a low and restricted energy supply and establish a relationship across wireless networks. While sensor networking and computing are high-speed, wide-ranging technologies, such as the automotive, war fields, medical, robots, weather and etc. may be conceived.

ISSN: 2005-4262 IJGDC

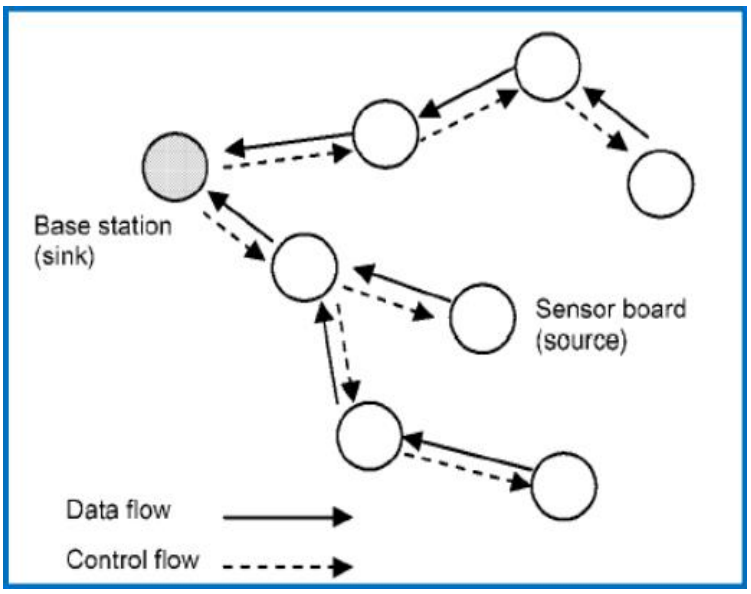

Fig. 2. An Example of the Data Flow in the Sensor Networks

Literature Review

Weidong Fang et. al. (2020) The knowledge protection of wireless network sensors (WSN) is a core component of the information sensing and aggregation phase for big data, cloud storage, and the Internet of Things (IoT). Becoming a soft target for many security threats due to the constrained resources of the sensor node. It is tougher to protect from internal threats than external attacks. Studies also shown that the technologies used to manage trust is an efficient way to monitor and protect against internal assaults. In addition, their benefits and weaknesses in the defense from internal threats are symmetrically contrasted and evaluated. Further detail is given on potential directions for confidence protection. The assumptions and outlook are finally given.

WiameBenzekri, Ali El Moussati, Omar Moussaoui, Mohammed Berrajaa (2020) Because of global warming, the danger of causing fires is raised mechanically. There is a growing amount of forest fires, which is increasing. The proposed framework would use artificial intelligence, especially Deep Learning (DL) models, to collect environmental network data from the forest and to predict forest fires. The combination of the Internet of Things (IoT) framework comprises a Low Power Large Area (LPWAN), fixed or mobile sensors and a strong model for deep learning. It is possible to demonstrate the viability of an autonomous and real-time environmental monitoring framework for complex risk factors of forest fires that different models focused on deep learning are being tested and compared.

ProsantaGope, Jemin Lee and Tony Q. S. Quek (2017) Wireless sensor networks (WSNs) include autonomous space-assigned devices which use sensors to monitor environmental and physical conditions. This standalone devices or nodes combine with routers or gateways for many real-time applications dependent on WSN. Until now, a lot has been achieved to design a lightweight, anonymous WSN real-time authentication protocol. Here is a way to fix do-strikes without compromise on anonymity help in the creation of lightweight anonymous authentication protocol for WSN-based real-time applications. We claim that we can effectively integrate our suggested approach into current DoS-resilient schemes.

Divya Acharya, ShubhLakshmiAgrwal, Pankaj Sharma and Sandeep Kumar Gupta (2016) Wireless Sensor Network is vulnerable to many security hazards like wormhole attack, playback or alteration of texts, spoofing of identification, black trole attack, eavesdropping and so on. The findings of networks that have a select forwarding attack then identification and deletion algorithm output are analysed. They are analyzed. The protection strategy succeeds dramatically in managing the attack thus restoring network efficiency and decreases the impact of network attack.

Guangjie Han, Jinfang Jiang, Lei Shu, JianweiNiu, Han-Chieh Chao (2014) Multiple protection risks may be faced via the Wireless Sensor Network (WSN) and conventional security measures cannot be implemented as a consequence of connectivity, computing and time limits of the WSNs. Models of confidence protection as an efficient protection framework for WSNs have been proposed lately. Furthermore, we categorize different forms of malicious attacks against models of confidence and examine whether current model trust can or cannot withstand them. Finally, we mentioned some best practice confidence practices that are critical for creating a good WSN trust model focused on both evaluations and contrasts.

Wireless Sensor Network

Routing and Security

Many WSN routing protocols exist and can be categorized into flat, hierarchical, location-based routing. We model location-based routing in this analysis, using a sensor node to assess routing physical place on the network. A subset of localized routing is gullible packet transfer, in which traffic often goes to the sink. We model a neighbor that is randomly closer to the sender node such that the sender node will randomly pick the nodes closer to the sink. This technique minimizes the precision of the details regarding neighbors and decreases the amount of transactions required for the sending of a packet.

Routing to accept a packet of data from a computer and to transmit the data to another device across the network on another network.

Routers, software and hardware, may be split into two major classes:

- **Hardware Routers**

The above routers are hardware that operates the particular applications the manufacturers create (currently they look just as black box). This program offers the routing capacity to move data from a network to another network as the most basic and maybe the essential job. Many businesses continue to use hardware routers because the hardware routers have a high speed and durability when contrasting software routers.

- **Software Routers**

With hardware routers the software routers have identical features, and the key purpose is to forward data from one network to another. An NT or Linux server may be a software router.

Network layer WSN dos attacks include routing knowledge alteration, selective transmission, sinkhole attack, Sybil attacks, and wormholes. Our emphasis is on selective forwarding, which declines to transmit such messages to a compromised node along the path, which are

dropped from the network and never enter the plunger. In the simplest scenario, a corrupted node resembles a black hole and ignores all packets. This is considered an assault with the black hole.

Many protocols for the network routing of sensors are very easy and therefore sometimes are more prone to target ad-hoc protocols in general. Many layer attacks on sensor networks fell into one of the groups below:

- Spoofed, altered, or replayed routing information
- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormholes
- HELLO flood attacks
- Acknowledgement spoofing

Defending DoS attacks from the network layer is an active research field. While a variety of algorithms are possible to identify black holes and other intrusions, they all have considerable overhead energy and difficulty. Many of these approaches would often become less efficient if multiple nodes in the network are infected or if a node uses smart selective transfers. Redundant messages routing through uncomplicated roads alleviates the possibility of node blockage, which is powerless and bandwidth unsustainable. Moreover, replication on a sparse network can be challenging or unlikely.

Coverage

The coverage issue, which indicates how well a field is being managed or monitored by sensors, is one of the major problems in WSN. Coverage depends on the manner in which the network connects with the landscape. We concentrate on the robustness of the network in the surveillance of a region during a DoS attack, so the coverage is the measure of our natural efficiency.

Provided a series of sensors S = s1,s2,...sn, in a twodimensionalzoneA, with each sensor si, I = 1,...,n, placed at a co-ordinate (xi,yi) in A and having the ri sensor range, if the sensor is within a range, the position in A should be protected by si.

One of the main challenges for WSN is the coverage challenge since it specifically impacts the use of resources and network existence of sensors. In general, the coverage issue may be how the network region is efficiently controlled.

Covery protocols may be closed to either connectivity-conscious coverage protocol or non-connectivity-conscious coverage protocols depending on the connectivities criteria. In addition, coverage protocols may be categorized in either distributed protocols or clustered protocols according to the algorithm characteristics adopted. Centralized coverage protocols can also be divided into evolutionary protocols (EA) or non-EA protocols. In addition, coverage protocols may be categorized by network model.

ISSN: 2005-4262 IJGDC

If the application plan does not obey a distribution of probabilities, it is not possible to track the statistical study. A particular methodology is required to find the optimum network configuration. The methodology we suggest is focused on the simulation of agents.

Experiments

A new cooperative networking scenario was applied in which a mobile robot extension of the wireless sensor network with self-healing ability is carried out by restoring its range where a disabled sensor falls in. Simulations were performed on an Intel Core i7 Processor 860 @ 2.80 GHze with 6GB of RAM under Windows 7 Home Premium and 64-bit architecture under Microsoft Robotics Development Studio (MRDS)2.By building a community of fixed platforms (in White), a territory perimeter around a vital infrastructure is generated as seen in the figure. 4. The brown node beyond the perimeter is an attacker who tries to impact the protected region. Each platform has a built-in battery-powered sonar system that facilitates immediate proximity monitoring. The ID of a platform is the same as the ID of a sensor only. The battery level and intrusion distance, along with a related risk perception, would consider two risk sources per applied platform. A snapshot of each platform documenting the function vector is processed every 60 ms centrally.

Fig. 3. The Simulated Outdoor Territorial Security Scenario

As the overall S sensing device danger goes above a permissible level (as seen in Fig. 5), in order to identify the attacker and to take more action, the mobile robot positioned on the periphery (see Fig. 4) can connect a S coordinate to its invitation and ultimately shift to protect the environment. The robot even recharges the sensor's power.

ISSN: 2005-4262 IJGDC

Fig. 4. Feature-Dependent and Overall Risk Assessment for Each Sensor in the Deployment Field

The original user-specified danger function modelling as seen in Fig. Six and seven. As the risk increases linearly with battery power decrease (Fig. 6), the trapezoidal component works in Fig. 7 shows that the perpetrator is at full bearing in a radius of 2 metres, which progressively disappears before after 3 metres. The graphical interface enables the consumer to use an alternate model shadow for any danger attribute, such that the corresponding μ threshold is set accordingly.

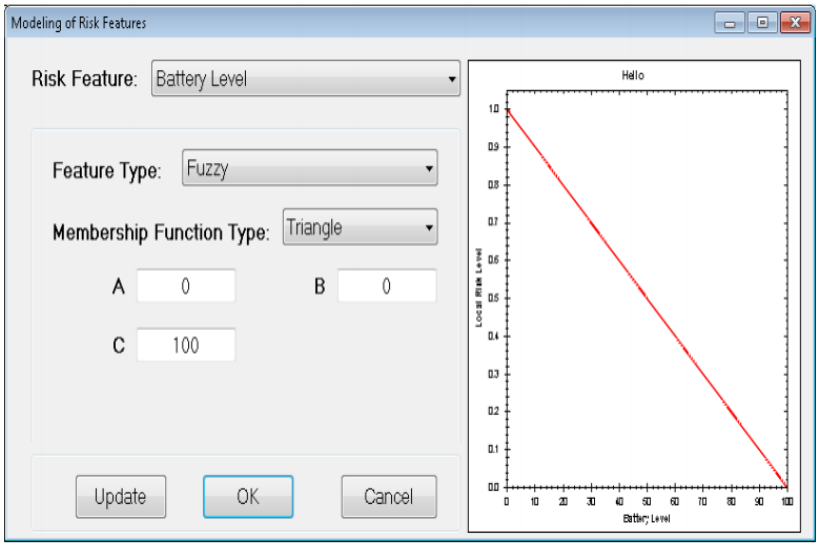

Fig. 5. Fuzzy Set Specification of the Battery Level Risk

ISSN: 2005-4262 IJGDC

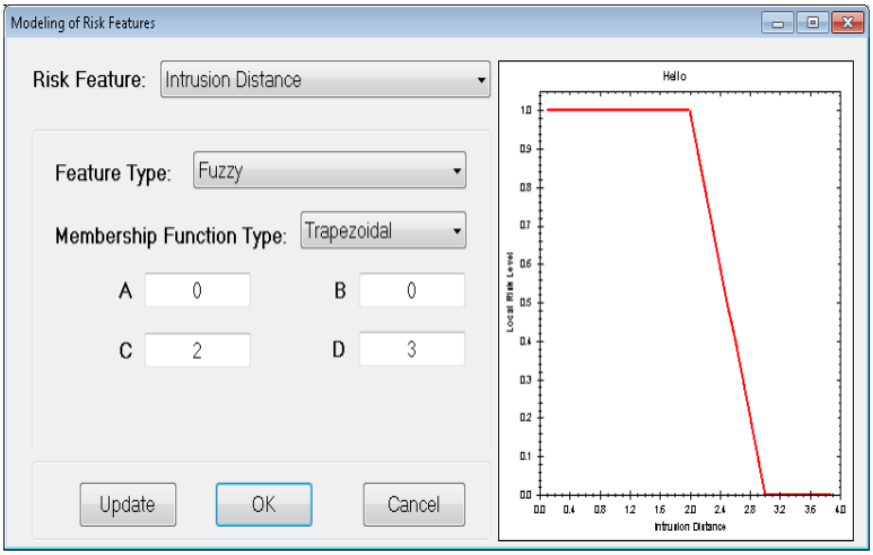

Fig. 6. Fuzzy Set Specification of the Intrusion Distance Risk

The risk visualization module controlled by the ESC algorithm provides visual input to the consumer on the operational complexities of the WSN in conjune with the internal risk appraisal of each device unit. During ESC's exercise, definition drifts and improvements are observed by contrasting the distributions of the clusters of the previous and current Sect-guided data snapshots. As seen in Fig. 8.

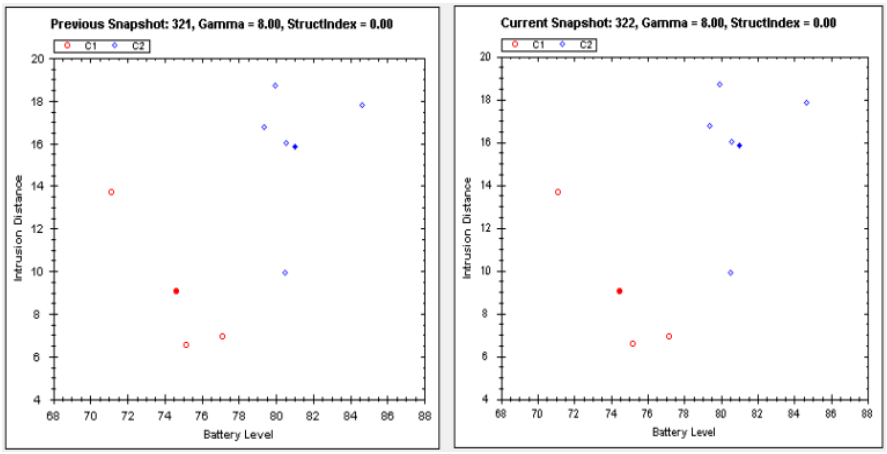

Fig. 7. Two Consecutive Data Snapshots Being Processed by the Evolving Shadowed Clustering (ESC) Architecture

The metrics of the cluster in Sect. The exposed configuration is diligently indicated by V-B2. Where there is an unusual occurrence in the device (e.g., the change to the irregular mode or the proximity of the attacker to the perimeter of the network) the precision, compactness and reliability of the affected clusters are automatically mirrored. Sect explains the mechanism of complex cluster creation. Through modifying the prototypes, setting or removing clusters,V-B3 can re-adjust the cluster allocation in order to obtain a consistent collection of information structures in the current snapshot. This is seen in the image 8.

ISSN: 2005-4262 IJGDC

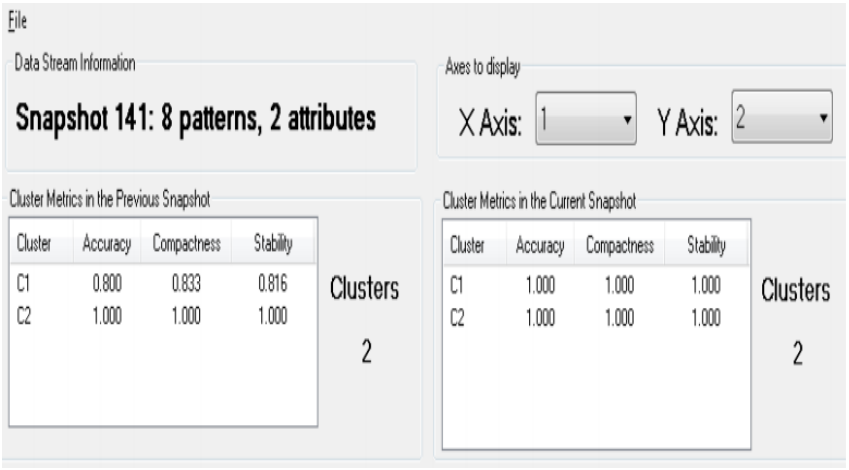

Fig. 8. Cluster-Related Metrics Computed by the ESC for Each Data Snapshot. Notice How the Loss of Stability in the Previous Snapshot for C_1 Has Been Overcome in the Current Snapshot By Means of the Dynamic Formation of Clusters, in This Case through the Update of the Clusters' Prototypes

The parameter list needed for ESC is shown in Table I. Their values were calculated after rigorous analytical study in which appropriate sample ranges were regarded for each of them.

Table I ESC Parameters

Parameter	Value	Description
M	**2**	
Tmax	**100**	
[Cmin; Cmax]	**[2;10]**	
ε^-	**0.4**	
ε^+	**0.33**	
ω	**0.4**	
N_1	**2**	

Conclusion

Safe routing is important for the wide-spread implementation of sensor networkes, linking layer encryption and authentication, multipath routing, identity confirmation, bilateral ties and authenticated broadcasting; protocol routing may be secured against aliens, forged routing details, sybil assaults, floods, and knowledge eavesdropping. The attacks in Sinkhole and wormhole raise the essential difficulties of routing protocols, which is that security mechanisms against such attacks are unlikely to occur since the creation of routing protocols. Protocols are challenging to build against these tow assaults. However, we should expect that harmony can be sought on the attacks with protocols like regional routing. Coverage in

wireless networks is generally characterized as the degree to which the sensors may observe their physical environment and for how long. In this paper we are analyzing the recent work in this sector in a representative way.

References

1. P. Porkar and M. Gheisari, "Performance analysis of two sensor data storages," presented at European Conference on Complex Systems 2011 (ECCS11), Tenerife, Spain, 2011.
2. A.Singla and R. Sachdeva, "Review on security issues and attacks in wireless sensor networks," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, issue 4, April 2013.
3. M. Chowdhury, M. F. Kader, and Asaduzzaman, "Security issues in wireless sensor networks: A survey," International Journal of Future Generation Communication and Networking, vol. 6, no. 5, pp. 97-116, 2013.
4. Wang, Y., G. Attebury, and B. Ramamurthy. 2006. "A Survey of Security Issues in Wireless Sensor Networks." IEEE Communications Surveys and Tutorials, 8(2): 2-23.
5. Pathan, A-S. K., Alam, M., Monowar, M., and Rabbi, F., "An Efficient Routing Protocol for Mobile Ad Hoc Networks with Neighbor Awareness and Multicasting", Proc. IEEE E-Tech, Karachi, 31 July, 2004, pp. 97-100.
6. WiameBenzekri, Ali El Moussati, Omar Moussaoui, Mohammed Berrajaa, "Early Forest Fire Detection System using Wireless Sensor Network and Deep Learning", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 5, 2020
7. Weidong Fang, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni, and Yinxuan Yang, "Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey", Wireless Communications and Mobile Computing, Volume 2020, Article ID 2643546, 20 pages
8. P. Gope, J. Lee, and T. Q. S. Quek, "Resilience of DoS attacks in designing anonymous user authentication protocol for wireless sensor networks," IEEE Sensors Journal, vol. 17, no. 2, pp. 498–503, 2017
9. D. Acharya, S. L. Agrwal, P. Sharma, and S. K. Gupta, "Performance analysis of detection technique for select forwarding attack on WSN," in 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 581–584, Waknaghat, India, December 2016.
10. Guangjie Han, Jinfang Jiang, Lei Shu, JianweiNiu, Han-Chieh Chao, "Management and applications of trust in Wireless SensorNetworks: A survey", Journal of Computer and System Sciences 80 (2014) 602–617
11. Kassim, M. R. M., & Harun, A. N. (2018). Wireless sensor networks and cloud computing integrated architecture for agricultural environment applications. Proceedings of the International Conference on Sensing Technology, ICST, 2017-Decem, 1–5.
12. Kumari, S., & Om, H. (2016). Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. Computer Networks
13. Kanagaraj, E., Kamarudin, L. M., Zakaria, A., Gunasagaran, R., &Shakaff, A. Y. M. (2015). "Cloud-based remote environmental monitoring system with distributed WSN weather stations" 2015 IEEE SENSORS - Proceedings
14. Sharma, V., R. Patel, H. Bhaduria, and D. Prasad. 2015. "Policy for random aerial deployment in large scale wireless sensor networks". In Computing, Communication & Automation (ICCCA), 2015 International Conference on, pp. 367–373, IEEE
15. C. M. Yu, Y. T. Tsou, C. S. Lu, and S. Y. Kuo, "Localized algorithms for detection of node replication attacks in mobile sensor networks," IEEE Transactions on Information Forensics and Security, vol. 8, no. 5, pp. 754–768, 2013.

ISSN: 2005-4262 IJGDC