Trends of Recent Secure Communication System and its Effectiveness in Wireless Sensor Network

Manjunath B E
Research Scholar
Jain University
Bangalore, India

P.V. Rao
Prof & Head of R&D, Dept. of Electronics & Communication Engg. RRCE
Bangalore, India

***Abstract*—Wireless sensor network has received increasing attention from the research community since last decade due to multiple problems associated with it. Out of many other significant problems e.g. routing, energy, load balancing, resource allocation, there is a lesser extent of effective security protocols towards solving security pitfalls in wireless sensor network. This paper studies the trend of research manuscript published in last six years about security problems to find that cryptographic techniques received more attention compared to non-cryptographic-based techniques. It also reviews the existing implementation towards addressing security problems and assesses its effectiveness by highlighting beneficial factor as well as limitations. Finally, we extract a research gap to identify the unexplored area of research, which is finalized to be implemented as a part of the future study to overcome the recent security issues.**

***Keywords*—Wireless Sensor Network; Security; Cryptography; Encryption; Secured Routing**

I. INTRODUCTION

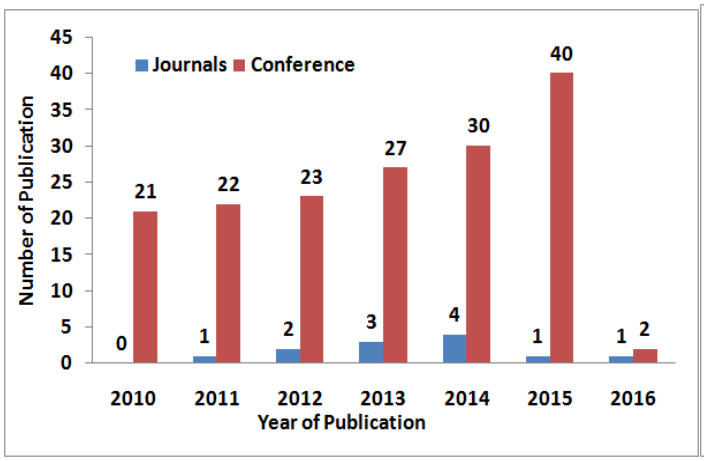
A wireless sensor network consists of wireless sensor nodes which disperse evenly (in small scale deployment) or randomly (in large scale deployment) to capture the specific environmental information and forward it to the user using base station. This process is called as data aggregation in wireless sensor network [1] [2]. The complete success rate of data aggregation depends on how efficiently the routing among the nodes takes place in presence of uncertain traffic scenario. There are three types of routing protocols in wireless sensor network i.e. flat, hierarchical, and hybrid [3]. While performing communication, sensor nodes will require considering all forms of issues e.g. routing issues [4], load balancing issues [5], resource allocation issues [6], security issues [7], energy issues [8], etc. Majority of the sensor nodes works on the principle of 1st order radio-energy model which associate a direct relationship with radio (communication) and energy (i.e. battery). A sensor node is also known to possess very limited computational capability, restricted battery, and less memory. Due to this, it is quite a difficult task to run recursive algorithms in a sensor node, especially on those which require performing monitoring for longer duration of time without any human intervention. The majority of the standard routing protocols are meant for improving communication performance and not the security features. Although, there are multiple forms of secure routing protocols e.g. [9] [10], these routing protocols are not meant for protecting all dimensions of attacks e.g. Sybil attack, Denial-of-Service attack, Wormhole attack, Sinkhole attack, node capture attack, statistical attack, replay attack, rushing attack, etc. There are various review papers discussing about existing security protocols in wireless sensor network [11]-[12], but the biggest challenges of those papers are i) they doesn't discuss the comparative analysis, which makes difficult to understand the best one, ii) majority part of the article has repetitive discussion of theory of sensor network and security which overshadows research contribution, and ii) they don't discuss explicitly the future work, which makes the reader vague to understand the contribution.

We actively comment that research on security problems in the sensor network is more than a decade old and still there are multiple underlying problems. There is a significant problem in existing techniques of Intrusion detection system [13] in WSN and identification of nodes are never studied in full fledge. There are multiple forms of possible nodes e.g. good nodes, attacker nodes, selfish nodes and partially defective nodes. It is said that differentiating all the above four categories of nodes is near to impossible for a given instant of time with heuristic routing data. It is because of the logic that when an attacker or malicious nodes intrudes a network by any means than it will never try to initiate an attack. Due to insufficient network and vital information from other nodes, the malicious nodes will not launch any form of attacks. In spite, it may start cooperating in data packet forwarding process just to accomplish more trust and reputation in the network. Because of this, differentiating a regular and malicious node is a challenging task. This is a very typical example to prove that existing techniques which are more inclined towards cryptographic usage, authentication mechanism, encryption, are not ultimately fruitful as in some point of time it could have missed identifying the intruders. Cryptographic techniques are quite expensive in implementation viewpoint, and existing methods don't bother about the practicality of the application of such technologies.

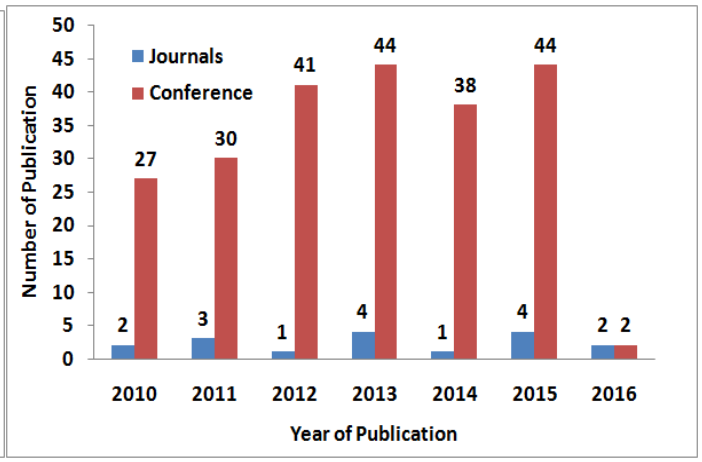
Therefore, the prime aim of this paper is to put forward the contribution of the research work being implemented during 2010-2016 towards thwarting the security issues in wireless sensor network. Section II discusses existing research trends on sensor network security followed by an explicit discussion of recent techniques in Section III. Research gap is explained in Section IV followed by the discussion of future work in Section V along with highlights of the tentative system architecture of it. The summary of the paper is discussed in Section VI.

II. Existing Research Trends on WSN Security

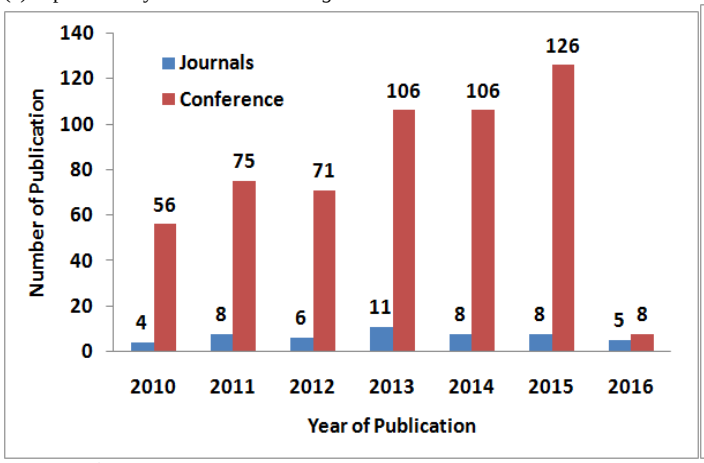
At present, there are multiple review papers e.g. to prove that security problems in wireless sensor network have received a good number of attentions from the researchers in till date. Some of the important review papers e.g. [14]-[15] have descriptively discussed the contribution of the research field of security problems. However, as the security concerns are unsolved till date, we conclude that it was quite a difficult task to understand the effectiveness of the existing techniques. We strongly believe that security features can be incorporated in multiple ways and it is not necessary to include cryptographic techniques only. A closer look at the research trends shown in Fig.1 will highlights that journals (or Transaction papers) found in reputed site IEEE Xplore is extremely less. Fig.1.(a)-Fig.(c) are more or less related to cryptographic attention where we can see that good numbers of research papers certainly do exists. However, Fig.1.(d) is based on trust and reputation-based security techniques which have very less number of implementation studies to date. There are only 6 journals published in IEEE based on trust and reputation based approach to secure the communication system in wireless sensor network. A similar trend can also be seen in other research-based publishers e.g. ACM, Springer, Elsevier, etc. Usually, the mechanisms that are designed based on Behavioral-based factors e.g. trust and reputations are much more light weight algorithms as compared to cryptographic techniques. However, it has received a poor attention. It should be known that wireless sensor node plays a chief role in advance technologies like Internet-of-Things (IoT) where existing security protocols are not that efficient. It will mean that IoT is a combination of cloud (Internet) and wireless sensor network which works on two different forms of security protocols. It will also mean that security protocols designs on the cloud are slightly incompatible to be executed over sensor nodes due to resource limitations. Hence, existing cryptographic protocols implemented on wireless sensor network will require an increasing attention in such cases. Implementing cryptographic applications will call for more resource consumption and larger management tools for associated security protocols which are expensive in nature. Hence, trust and reputation based techniques are the only solution of defense which doesn't require any additional resource or any dependency of complex key management or sophisticated encryption. Therefore, there is a need of investigating non-cryptographic algorithms for the optimal security keeping the future generation of sensor network usage.



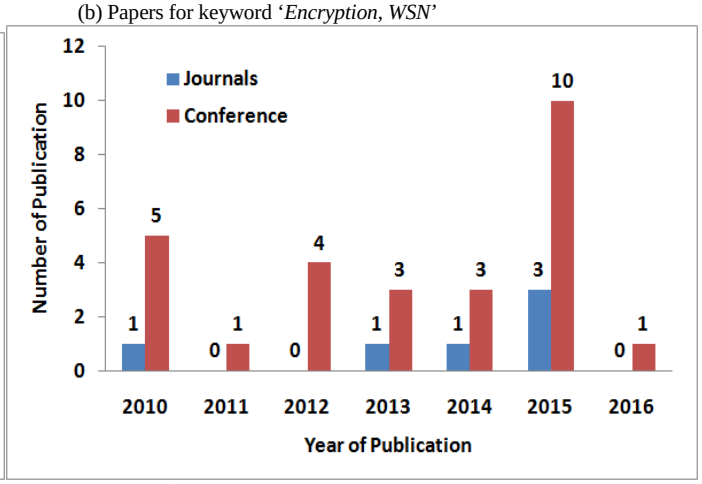
(a) Papers for keyword '*Secure routing in WSN*'



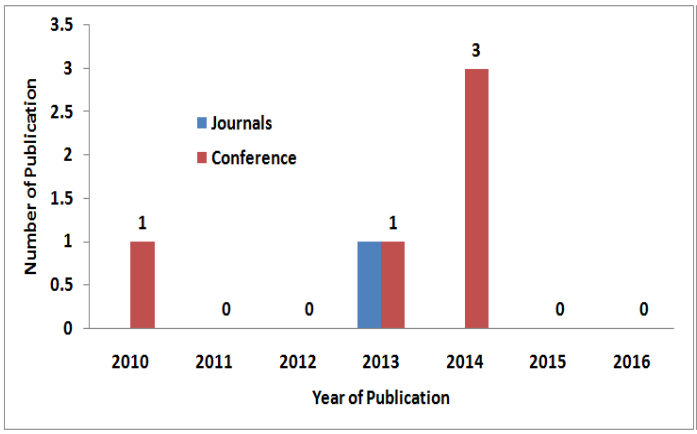
(b) Papers for keyword '*Encryption, WSN*'



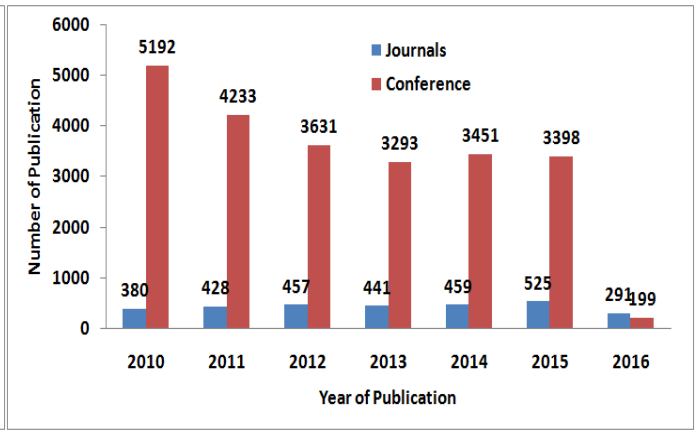
(c) Papers for keyword '*attacks, WSN*'



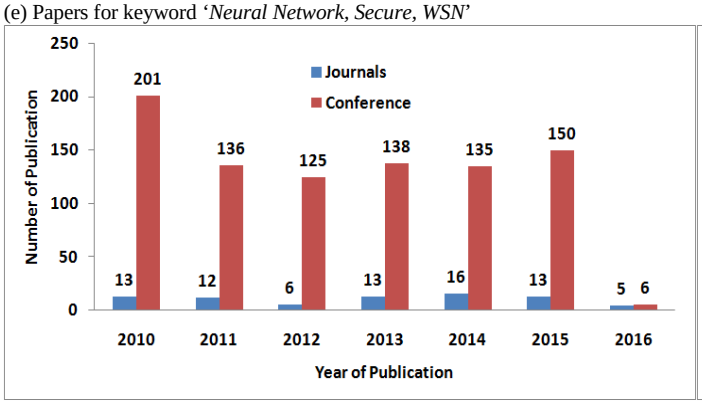
(d) Papers for keyword '*trust, reputation, WSN*'



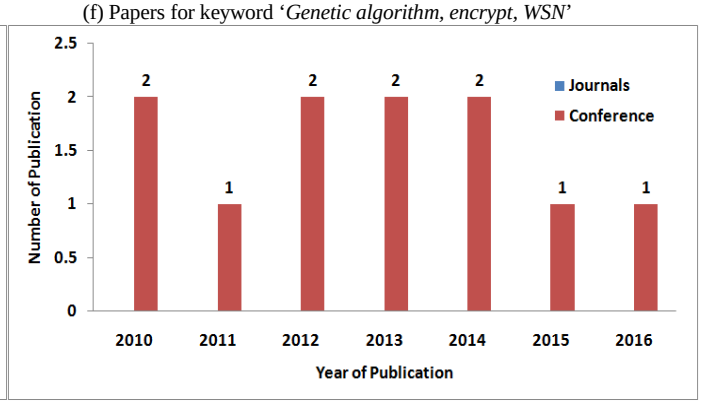
(e) Papers for keyword '*Neural Network, Secure, WSN*'



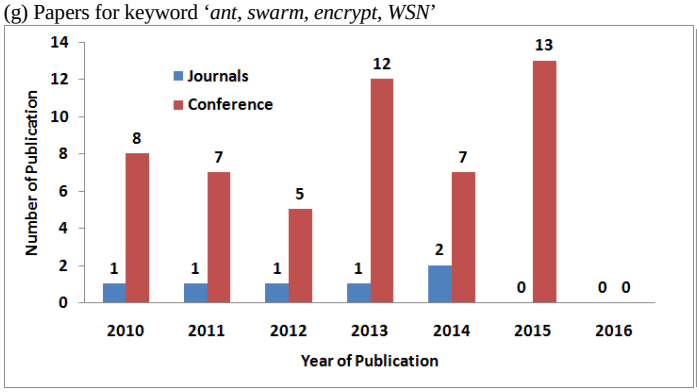
(f) Papers for keyword '*Genetic algorithm, encrypt, WSN*'



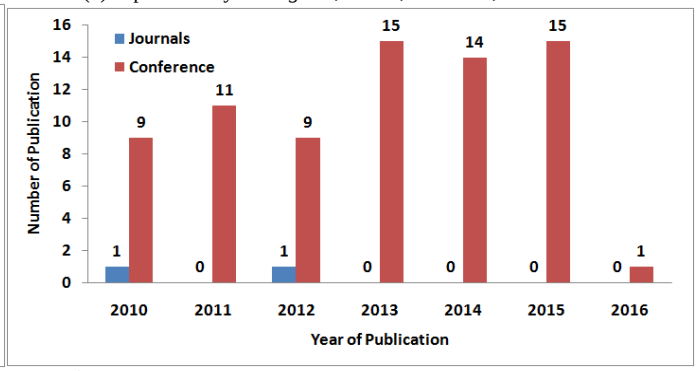
(g) Papers for keyword '*ant, swarm, encrypt, WSN*'



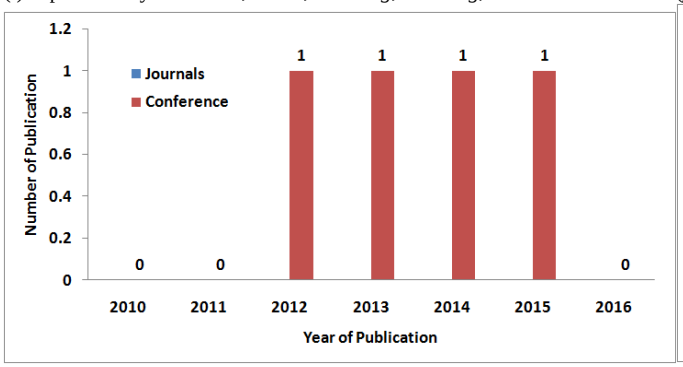
(h) Papers for keyword '*game, secure, malicious, WSN*'



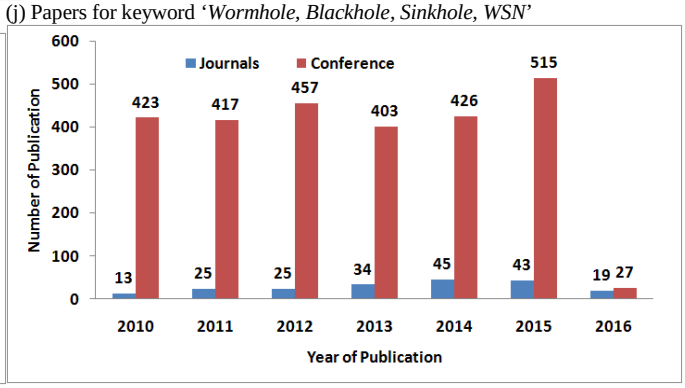
(i) Papers for keyword '*DoS, DDoS, Jamming, Flooding, WSN*'



(j) Papers for keyword '*Wormhole, Blackhole, Sinkhole, WSN*'



(k) Papers for keyword '*node capture attack, brute force, byzantine, WSN*'



(l) Papers for keyword '*rushing, replay, routing, WSN*'

Fig. 1. Trends of Research Publication for Security in Wireless Sensor Network between 2010-2016

III. RECENT TECHNIQUES

At present, there are dozens of research papers which has reviewed the existing security protocols in WSN. Hence, to avoid repetitive discussion, we discuss only the recent studies manuscript published during the year of 2010-2016. For productive discussion, we classify the techniques in three forms i.e. i) routing-based security methods, ii) cryptographic-based security techniques and iii) optimization-based security techniques. We only discuss the papers which are found to provide a solid base of security implementation in WSN most recently.

A. Routing-based Security Techniques

The routing based security techniques normally implement the Security features during performing routing operation. In such cases, the existing routing techniques are suitably modified to ensure security. Most recently, Das et al. [16] have presented a routing technique to resist wormhole attack as well as flooding attack in WSN. The method uses MAC scheme with the main management to ensure security. Nandu and Shekokar [17] have presented an authentication technique to resist DoS attack in WSN. The technique has used the concept of re-programming to do so. Re-programming is a mechanism of performing a selection of scope, decoding-encoding, versioning, etc. Henze et al. [18] have developed a secure access policy to protect sensitive sensor data over cloud environment. The study outcome shows minimization of key exchange time. The technique also uses AES encryption using 128 bit of key size as well as RSA with 2048 bit keys. Chen and Chen [19] have enhanced LEACH protocol suitable to incorporate security features. Considering the mobility of the nodes, the technique alters the clustering accordingly. The study outcome was compared with LEACH on energy, memory consumption, etc. Menaria et al. [20] have presented a unique algorithm for identifying the location of compromised node in WSN. The technique is used for isolating the compromised and misbehaved nodes from the network. The technique also uses Wiener index spanning tree to compute energy efficiency, and its outcome was evaluated on packet drop, energy, and throughput. Mengyao et al. [21] have developed a technique using ring-based grouping mechanism in WSN. The technique was meant for securing inter-cluster communication whose security depends on the trust factor. Tang et al. [22] have introduced a CASER (Cost-Aware Secure Routing) in WSN. The technique is developed based on energy stability factor and random walking model using probability theory. The study outcome showed better communication performance. Masdari et al. [23] have presented a technique to evaluate an effectiveness of Secured LEACH protocol in WSN. Ferng and Rachmarini [24] have introduced a method of the energy-efficient communication system over grid topology using simple key management techniques. Obaidat et al. [25] have presented a method for securing heterogeneous WSN. Using the concept of the trust factor, the presented technique evaluated link quality and node quality based on distance, energy, etc. Hence, it can be seen that there are various forms of routing technique to secure WSN communication system but the focus is more biased on energy efficiency.

B. Cryptographic-based Techniques

This is another frequently used technique to perform security. The cryptographic method usually performs encryption mechanism on the vulnerable links or susceptible sensors to secure communication. However, it should be known that majority of the cryptographic protocols are old and hence the existing researchers chooses either to enhance the older or to develop a new one. The most recent study presented by Shankar et al. [26] has used public-key cryptography to secure communication system in WSN taking the case study of the healthcare sector. The technique uses Elliptical Curve Cryptography to perform mutual authentication. Munivel and Ajit [27] have used public key infrastructure to perform encryption and key management. Soosahabi et al. [28] have introduced a probabilistic cryptographic approach to understanding the state of transmission (to be a harmless or harmful state). Al-Haija et al. [29] have presented a cryptographic technique that uses RSA for the smaller scale of the sensor network. The approach was also experimental-based, and the outcome was evaluated with respect to time. Kodali and Sarma [30] have used Elliptical Curve Cryptography along with Diffie-Hellman key exchange protocol in WSN. Xu and Dang [31] have presented a technique that is resistive against Denial-of-Service attacks in WSN. The method uses joint implementation of Elliptical Curve Cryptography with a digital signature. Yan and Shu [32] have used AES protocol to obtain energy efficient cryptographic operation in wireless body area network. The author has developed an analytical model, and its outcome was studied on energy only. Jeon et al. [33] have presented a scheme which uses free surrounding resources to incorporate encryption policy. The technique was claimed to offer lowered complexity and better modulation method. Huang et al. [34] have presented a simple encryption scheme to safeguarding data aggregation in a sensor network. Liu et al. [35] have illustrated a unique signature scheme based on the identity of nodes using experimental approach.

C. Optimization-based Techniques

Usage of optimization has seen increasing attention from the year 2010 onwards. Most recently, there are multiple techniques of optimization adopted by the researcher. Narad and Chavan [36] have used a neural network to formulate a new authentication mechanism in WSN. The author has used Shamir Secret Sharing to perform encryption. Karapistol and Economides [37] have adopted game theory to address jamming attack in WSN. The attack environment was modeling using Bayesian Stackelberg games where the outcome was studied on probability and utility factor. The same authors have presented a different work in the same year [38] for performing anomaly detection. Kumar et al. [39] have jointly used the neural network and game theory to formulate a novel defense mechanism in WSN. Alrajeh et al. [40] have presented a bio-inspired algorithm to maintain secured communication in WSN. The technique uses Ant colony optimization, and its outcome was testified using efficiency of data forwarding and packet loss. Branch et al. [41] have presented a technique of simple optimization of in-network to perform outlier detection. Another implementation of game theory was carried out by Ding et al. [42]. The method

establishes the relationship between the resource utilization and vulnerable situation. The technique is evaluated on probability of selfish node discovery. Ramesh et al. [43] have presented a study that uses the neural network to resist DoS attack in WSN. The study outcome was evaluated using computational energy required to perform ciphering, memory consumption and execution time. Marmol and Perez [44] have discussed a new bio-inspired algorithm. The technique uses both reputation and trust factor using ant colony optimization. Estiri and Khademzadeh [45] have adopted game theory to perform intrusion detection. The method also assists in formulating defense strategies.

Hence, it can be seen that there are various techniques that call for inclusion of multiple methods for incorporating security features in WSN. The scale of the effectiveness of all the above-mentioned methods is tabulated in Table.1.

TABLE I. SUMMARIZATION OF RECENT TECHNIQUES OF SECURITY IN WSN

	Authors	Techniques	Advantage	Limitation
Routing-Based Security technique	Das et al. [16]	MAC-based authentication	-Resistive against Wormhole attack -energy efficient	-No discussion of computational complexity.
	Nandu [17]	Re-programming	-Faster Authentication	-No Benchmarking --No discussion of computational complexity.
	Henze et al. [18]	Re-programming, AES, RSA	Robust security over cloud	-Highly dependent on library -Storage / transmission overhead
	Chen [19]	Enhanced LEACH	-Energy Efficient	-Applicable to small networks -Not benchmarked with secure routing techniques.
	Menaria et al. [20]	Position Identification of compromised node, spanning tree	-Energy Efficient -Better communication	-No Benchmarking -No discussion of computational complexity.
	Mengyao et al. [21]	Ring-based clustering, trust, ant colony optimization	-Energy Efficient	-No Effective Benchmarking -No discussion of computational complexity.
	Tang et al. [22]	Cost-Aware Secure Routing	-Energy Efficient -Resistive against trace back attacks in routing	-No Effective Benchmarking -No discussion of computational complexity.
	Masdari et al. [23]	Evaluation of Secure-LEACH	-Supportability of extensive cryptographic mechanism -Supports broadcast authentication,	-less supportability of message freshness, and pairwise authentication except few of them
	Ferng and Rachmarini [24]	Grid-based, simple key management	-Energy Efficient	-Not applicable to dynamic networks -Not resilient against any major lethal threats in WSN
	Obaidat et al. [25]	Dynamic energy, heterogeneous WSN	-Energy Efficient	-Overhead discussion is not made
Cryptographic-Based Security technique	Shankar et al. [26]	Elliptical Curve Cryptography	-Smaller Key Size	-No Effective Benchmarking -No discussion of computational complexity.
	Munivel and Ajit [27]	Micro-Public Key Infrastructure	-Energy Efficient	-No Effective Benchmarking -No discussion of computational complexity.
	Soosahabi et al. [28]	Probability theory,	-Effective against statistical attacks	-No Effective Benchmarking -No discussion of computational complexity -Consumes Resources
	Al-Haija et al. [29]	RSA	Robust Encryption for smaller scale network.	-Not a lightweight encryption -Not applicable for large scale network
	Kodali and Sarma [30]	ECC, Diffie-Hellman	-Robust Encryption -Resilient against Brute-force attack	-Not Energy efficient
	Xu and Dang [31]	ECC, Digital Signature	-41% of energy minimization -resistive against DoS attack	-No Effective Benchmarking -No discussion of computational complexity
	Yan and Shu [32]	AES	-Energy Efficient	-No Effective Benchmarking -No discussion of computational complexity
	Jeon et al. [33]	Encrypted fusion rules	-Lowered error probability	-No Effective Benchmarking -No discussion of computational complexity
	Huang et al. [34]	Key-verification	-Simple authentication of key.	-Less Effective key management. -Lead to communication overhead -less Security strength
	Liu et al. [35]	Signature-based	-Supports both online and offline	-No Effective Benchmarking

			verification. -Suitable for large area.	-No discussion of computational complexity -Signature generation and validation doesn't conform to backward secrecy.
Optimization-Based Security technique	Narad and Chavan [36]	Neural network, Shamir Secret Sharing	-maintains message integrity	-No Effective Benchmarking -No discussion of computational complexity
	Karapistol and Economides [37]	Game theory	-resistive against jamming attack.	-No Effective Benchmarking -No discussion of computational complexity
	Karapistol and Economides [38]	Anomaly detection using ruleset	-Higher accuracy of attack detection	-Communication performance nor evaluated.
	Kumar et al. [39]	Game theory, neural Network	-60% accuracy in attack detection	-Theoretically sound but no evidence of practical implementation.
	Alrajeh et al. [40]	Ant colony optimization	-need less time to forward data -better communication performance	-No evidence of scalability -No Effective benchmarking
	Branch et al. [41]	Non-parametric optimization, outlier detection	-energy efficient	-Not secure against passive attacks
	Ding et al. [42]	Game theory	Detection of intrusion based on resource consumption	-The model doesn't have validation in uncertainty. -Low scope of utility function. -Less practical implementation
	Ramesh et al. [43]	Neural Network, symmetric key algorithm	-Resistive against DoS attack	-Leads to excessive iteration -Less effective classification of intrusion..
	Armol and Perez [44]	Ant colony optimization, trust, reputation	-energy efficient	-Not compliant of space complexity
	Estiri and Khademzadeh [45]	Game theory	-better intrusion identification	-No evidence of scalability -No Effective benchmarking

IV. RESEARCH GAP

After reviewing the existing techniques and solutions offered by the researchers till date, it can be just inferred that existing techniques have both potentials and pitfalls. The potential beneficial factor of the existing techniques discussed in previous sections only shows they are more inclined to accomplish energy efficiency while implementing security protocols. However, sometimes the energy efficiency is obtained at the cost of overlooking security aspects in full dimensional of vulnerability. It was also observed that existing mechanism are too much symptomatic in nature on attacks. It will mean that solutions design for mitigating DoS attack is not even capable of identifying other forms of intrusion. It should be known that existing mechanism of routing and clustering in wireless sensor network involves mobility and dynamic topologies too which calls for multiple attacks with an uncertain or unpredictable pattern of intrusion. Hence, existing mechanism is not able to cater up to the first line of defense itself purely, which is just about identifying uncertain forms of attacks or hideous security breach. Moreover, existing solutions don't offer full fledge compliance towards integrity, privacy, anonymity, confidentiality, non-repudiation, availability, etc.

Moreover, we have seen that there are few benchmarked works published in 2010-2016 about security in wireless sensor network. We also find that studies are more on cryptographic usage ignoring the fact that a sensor can only process 48 kilobytes of physical memory. Existing optimization techniques are good attempt, but they are less practical in real-world motes. Optimization techniques based game theory sound good in theory, but its formulation cannot be judged to be potential until and unless there is any benchmarked work or designed using experimental study of large-scale sensor deployment. The significant research gaps found after reviewing the existing system are briefed as follows:

- Ignorance to Explore Best Secure Route: The existing standard secure routing protocols (e.g. Sec LEACH, Sec Rout, and HEED), etc. are developed over a similar network, which has less supportability of the multipath routing technique. It was also explored that existing security technique also could not address the research gap among reliable routing with energy and quality of service. In this regards, multipath routing is the only way to ensure a better level of tolerance against any critical fault owing to any physical attacks in wireless sensor network. It is also known that usage of multipath routing supports heterogeneous networks as well as it also invites a massive problem owing to the presence of Duplicated Routing Data (DRD). An adversary can compromise such DRD using malicious eavesdropping and can easily insert its malicious code that is its replicated version. Such codes can easily go without any validation. The consequences of intrusions through multipath propagation in wireless sensor network will be quite collateral in nature. The existing techniques are not found to solve such issues most recently.
- Narrowed Scenario of implementation: Normally the wireless sensor network is always studied with respect to static nodes and mobility factor is concern only with the sink nodes. But there are many possibilities of upcoming applications where the sensors may go mobile. In such scenario, if a node in heterogeneous wireless sensor network go on mobile than there may be massive energy consumption owing to radio transmission. The scenario may turn more worst if there are selfish nodes as they will not be ready for spending

more energy in assisting other data packet forwarding. Such forms of scenario will easily welcome all sorts of routing attacks, replay attack, wormhole attack etc. Availability of an intermediate node is extremely important in heterogeneous network as compared to homogeneous networks. The allowance of such intrusion will further lead to a unstabilized network that may highly degrade the communication performance along with stealing of data. Hence, even after the knowledge of mobility factor, IoT, ubiquitous computing, the researchers have not considered broader spectrum of recent problems and its implementation requirements.

- Resiliency against Potential Threats: In the area of healthcare or nuclear plant monitoring system, if the transmission line is not secured, it may cost the life of somebody. There are various hazardous and adverse condition of network deployment that results in unauthorized access to private details of sensor nodes. Although, with an aid of the model description in Section 2.2, we have seen that usage of cryptography can render further security. But the fact still remains unsolved are that "*Is the system resistive enough against brute force attack?*" The question is quite difficult to crack as brute force attack may lead to decryption of ciphered information using malicious code with infinite computing resources, which is highly possible. We have already seen that existing system are more inclined to achieve energy efficiency and there is a bit of imbalance between energy efficiency and security potential.

V. FUTURE WORK

Based on the research gap discussion in previous section, our future direction of the work will be focused towards cost effective security protocols in wireless sensor network. Our future work will be towards designing a mathematical modelling for analyzing an availability of best secure route. The work to be carried out in this regards are as follow:

- Adversarial Model: The study considers essential physical attack (e.g. node capture attack) as an insider attack model. However, novelty is incorporated in this adversarial modelling, where we consider the facts of resource expenses too. Hence, adversarial node with less resource will perform different action compared to an adversarial node with high resource. We will also model for uncertain behaviour for the adversarial node.

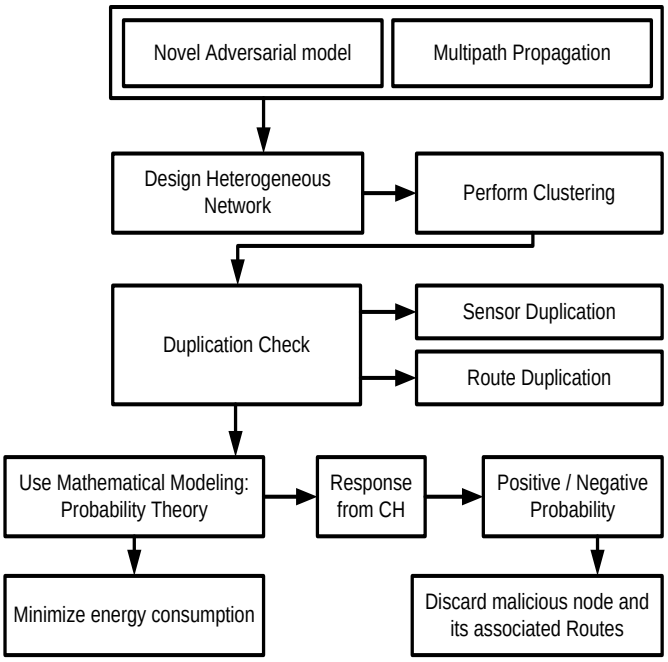


Fig. 2. Tentative System Architecture

- System Design: A simulation study of heterogeneous nodes with clustering process will be carried considering clusterhead and sensor node. The node distribution is carried out using random process. The novelty in the clustering process is that clustered area is not circular like in existing studies; they are more asymmetric in shape, which normally happens in real-time implementation. The system checks for duplication for both sensors and routes over multihop propagation. The design of the mathematical modelling will be entirely carried out by probability model. The system also checks for the positive / negative probability of a node / route being a malicious. Hence, a novel distributed election mechanism will be developed that can identify the malicious nodes. The mechanism will be initiated by random selection of neighbor nodes located near to monitored node. This process is carried out by all the clusterhead, which after computation shares its response using pairwise key. When maximum response is found to be negative for monitored node, it will be considered as malicious and hence will be discarded from the routing process. However, the process is quite bulky and may consume more energy, therefore, we will not be using conventional radio-

energy model and will chose to reformulate energy-based modelling where energy will be computed for performing security operations and not for normal routing and clustering operations. The tentative architecture is showcased in Fig.2

- Benefit: The benefits of the proposed system are as follows: i) the system doesn't use any forms of cryptography, which ensures that there is no complex computation process involved within a node. ii) The system uses probability theory for formulating a model in order to identify the suspicious sensors and routes along with less usage of energy of a node. iii) The identification of the response generated from CH is scaled positive / negative along with check for reliability that makes the detection and avoidance of the attackers highly precise.

VI. Conclusion

A better version of security protocols calls for inclusion of privacy, integrity, non-repudiation, anonymity, confidentiality factors. However, till date there is no single security algorithm in wireless sensor network which has maintained all of them in its security deployment among the nodes. One reason for it is basically the types of the nodes which are less capable of computational processing and other reason is the flawed design of security protocols. It was also seen that adoption of cryptographic technique is much high compared to non-cryptographic techniques. There is a benefit of using cryptographic technique which is robust authentication, but cryptographic implementation is generally recursive in nature and calls for multiple rounds of operation in order to perform encryption. Hence a good amount of memory and resource is required for this, which are the major pitfalls. Usage of non-cryptographic techniques is carried out mainly using probability theory and statistics. However, success rate of such usage depends upon the mathematical modelling. Last 6 years has found few implementations in the form of mathematical modelling. Therefore, our future work is dedicated to develop such a mechanism that will use a mathematical modelling and whose entire operation will permit identification of uncertain nodes and is capable to address the most difficult forms of adversaries in sensor network.

References

[1] S.Kaur, and M. Kaur, "Improvement In MAODV Protocol Using Location Based Routing Protocol", In MATEC Web of Conferences, vol. 57. EDP Sciences, 2016.

[2] J. Ma, W.Lou, and X-Y. Li, "Contiguous link scheduling for data aggregation in wireless sensor networks", Parallel and Distributed Systems, IEEE Transactions, Vol.25, No. 7, pp.1691-1701, 2014.

[3] A.G. Khan, A. Rahman, and N. Bisht, "Classification of hierarchical based routing protocols for wireless sensor networks", International journal of innovations in engineering and technology, pp.2319-1058, 2013

[4] S. Anbumalar, S. Prabhadevi, "A Survey On Routing Issues And Routing Protocols In WirelessSensor Networks", International Journal Of Engineering And Computer Science, Vol. 4, Issue. 6, pp. 12927-12931, 2015

[5] F. Bouabdallah, N. Bouabdallah, and R. Boutaba, "Load-balanced routing scheme for energy-efficient wireless sensor networks", In Global Telecommunications Conference, IEEE Globecom, pp. 1-6, 2008.

[6] M. Chitnis, P. Pagano, G. Lipari, and Y. Liang, "A survey on Bandwidth resource Allocation and Scheduling in wireless sensor networks", In Network-Based Information Systems, 2009. NBIS'09. International Conference, pp. 121-128, 2009.

[7] Q. Wang, and T. Zhang, "A survey on security in wireless sensor networks. Security in RFID and Sensor Networks",2009

[8] F. Chen, F., L. Guo, and C. Chen, "A Survey on Energy Management in the Wireless Sensor networks", IERI Procedia, Vol. 3, pp.60-66,2012.

[9] R. Selvam, and A. Senthilkumar, "Cryptography based secure multipath routing protocols in wireless sensor network: a survey", In Electronics and Communication Systems (ICECS), International Conference,pp. 1-5, 2014.

[10] A.M. E-Semary, and M.M.A. Azim, "A two-tier energy-efficient secure routing protocol for Wireless Sensor Networks", In Information Assurance and Security (IAS), 2011 7th International Conference, pp. 331-337, 2011.

[11] Y. Arfat, and R.A. Shaikh, "A Survey on Secure Routing Protocols in Wireless Sensor Networks",2016.

[12] S. Renubala, and K. S. Dhanalakshmi, "Trust based secure routing protocol using fuzzy logic in wireless sensor networks", In Computational Intelligence and Computing Research (ICCIC), IEEE International Conference, pp. 1-5, 2014.

[13] S. Athmani, D.E. Boubiche, and A. Bilami, "Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs", In Computer and Information Technology (WCCIT), 2013 WorldCongress, pp. 1-5, 2013.

[14] V. Kumar, A. Jain, and P.N. Barwal, "Wireless sensor networks: security issues", challenges and solutions. International Journal of Information & Computation Technology, ISSN, pp.0974-2239,2014

[15] Q. Yang, X. Zhu, H. Fu, and X. Che, "Survey of security technologies on wireless sensor networks", Journal of Sensors, 2015

[16] A.K.Das, R.Chaki, and K.N.Dey, "Secure energy efficient routing protocol for wireless sensor network", Foundations of Computing and Decision Sciences, Vol. 41, No. 1, pp.3-27,2016.

[17] P.Nandu, and N. Shekokar, "An Enhanced Authentication Mechanism to Secure Re-programming in WSN", Procedia Computer Science, Vol. 45, pp.397-406, 2015.

[18] M. Henze, S. Bereda, R. Hummen, and K. Wehrle, "SCSlib: Transparently accessing protected sensor data in the cloud. Procedia Computer Science, Vol.37, pp.370-375, 2014.

[19] L. Chen, "An Improved Secure Routing Protocol Based on Clustering for Wireless Sensor Networks", InMechatronics and Automatic Control Systems, pp. 995-1001, 2014 Publishing.

[20] V.K. Menaria, D. Soni, A. Nagaraju,S.C.Jain, "Secure and energy efficient routing algorithm for wireless sensor networks", InContemporary Computing and Informatics (IC3I), International Conference, pp. 118-123, 2014

[21] L. Mengyao, Y. Zhang, and X. Li, "Ring-based security energy-efficient routing protocol for WSN", In Control and Decision Conference, The 26th Chinese, pp. 1892-1897, 2014

[22] D. Tang, T.Li, J. Ren, and J. Wu, "Cost-Aware Secure Routing (CASER) Protocol Design for Wireless Sensor Networks", Parallel and Distributed Systems, IEEE Transactions, Vol. 26(4), pp.960-973, 2015

[23] M. Masdari, S.M. Bazarchi, and M. Bidaki, "Analysis of secure LEACH-based clustering protocols in wireless sensor networks", Journal of Network and Computer Applications, 36(4), pp.1243-1260, 2013.

[24] H.W. Ferng and D. Rachmarini, "A secure routing protocol for wireless sensor networks with consideration of energy efficiency", In Network Operations and Management Symposium (NOMS), IEEE, pp. 105-112, 2012

[25] M.S. Obaidat, S.K. Dhurandher, D. Gupta, N. Gupta, and A. Asthana, "DEESR: dynamic energy efficient and secure routing protocol for wireless sensor networks in urban environments",Journal of Information Processing Systems, Vol.6(3), pp.269-294, 2010

[26] S.K. Shankar, A.S. Tomar, and G.K. Tak, "Secure Medical Data Transmission by Using ECC with Mutual Authentication in WSNs", Procedia Computer Science, Vol. 70, pp.455-461,2015

[27] E. Munivel, and G. M. Ajit, "Efficient public key infrastructure implementation in wireless sensor networks", In Wireless Communication and Sensor Computing, ICWCSC, InternationalConference, pp. 1-6. IEEE, 2010.

[28] R. Soosahabi, Naraghi-Pour, D. Perkins, and M.A. Bayoumi, "Optimal probabilistic encryption for secure detection in wireless sensor networks. Information Forensics and Security",IEEE Transactions on, 9(3), pp.375, 2014

[29] Q.A. A-Haija, A. Tarayrah, H. A-Qadeeb, and A. Al-Lwaimi, "A tiny RSA cryptosystem based on Arduino microcontroller useful for small scale networks. Procedia Computer Science, Vol.34,pp.639-646,2014

[30] R.K. Kodali, and N.N. Sarma, "Energy efficient ECC encryption using ECDH", In Emerging Research in Electronics, Computer Science and Technology Springer, pp. 471-478, 2014

[31] J. Xu, and L. Dang, "Multi-User Broadcast Authentication Protocol in Wireless Sensor Networks against DoS Attack", Open Cybernetics & Systemics Journal, Vol.8, pp.944-950, 2014

[32] Y. Yan, T. Shu, "Energy-efficient In-network encryption/decryption for wireless body area sensor networks", InGlobal Communications Conference (GLOBECOM), IEEE 2014,pp. 2442-2447, 2014

[33] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks", Information Forensics and Security, IEEE Transactions, Vol.8, No. 4, pp.619-625, 2013

[34] S.I. Huang, S. Shieh, and J.D. Tygar, "Secure encrypted-data aggregation for wireless sensor networks. Wireless Networks, 16(4), pp.915-927, 2010

[35] J.K. Liu, J. Baek, J. Zhou, Y. Yang, and J.W. Wong, "Efficient online/offline identity-based signature for wireless sensor network. International Journal of Information Security, vol.9(4), pp.287-296, 2010

[36] S. Narad and P. Chavan, "Cascade Forward Back-propagation Neural Network Based Group Authentication Using (n, n) Secret Sharing Scheme", Procedia Computer Science, Vol. 78, pp.185-191,2016.

[37] E. Karapistoli, and A.A. Economides, "Defending jamming attacks in wireless sensor networks using stackelberg monitoring strategies",In Communications in China (ICCC), pp. 161-165, 2014

[38] E. Karapistoli, and A.A. Economides, "ADLU: a novel anomaly detection and location-attribution algorithm for UWB wireless sensor networks", EURASIP Journal on Information Security,pp.1-12, 2014.

[39] E.S. Kumar, S.M. Kusuma, and B.V. Kumar, "An intelligent defense mechanism for security in wireless sensor networks", In Communications and Signal Processing (ICCSP), pp. 275-279, 2014.

[40] N.A. Alrajeh, M.S. Alabed, and m.S. Elwahiby, "Secure ant-based routing protocol forwireless sensor network", International Journal of Distributed Sensor Networks, 2013.

[41] J.W. Branch, C.Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks", Knowledge and information systems, Vol.34(1), pp.23-54, 2013

[42] Y. Ding, X.W. Zhou, Z.M. Cheng, and F.H. Lin, "A security differential game model for sensor networks in context of the internet of things. Wireless personal communications, Vol.72(1), pp.375-388, 2013.

[43] 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, pp. 783-787, 2012

[44] F.G. Mármol and G.M. Pérez, "Providing trust in wireless sensor networks using a bio-inspired technique. Telecommunication systems, Vol. 46(2), pp.163-180, 2011

[45] M. Estiri, and A. Khademzadeh, "A game-theoretical model for intrusion detection in wireless sensor networks. In Electrical and Computer Engineering (CCECE), 23rd Canadian Conference, pp. 1-5, 2010