International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 2, April 2018, pp. 1048~1055
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i2.pp1048-1055

Balancing Trade-off between Data Security and Energy Model for Wireless Sensor Network

Manjunath B. E.[1], P. V. Rao[2]
[1]Dept. of ECE, Jain University, Bangalore, India
[2]Dept. of ECE, VBIT, Hyderabad, India

Article Info

Article history:

Received Sep 7, 2017
Revised Jan 6, 2018
Accepted Jan 16, 2018

Keyword:

HMAC
Pair-wise key establishment
Security
WSN

ABSTRACT

An extensive effort to evolve various routing protocol to ensure optimal data delivery in energy efficient way is beneficial only if there is additional means of security process is synchronized. However, the security process consideration introduces additional overhead thus a security mechanism is needed to accomplish an optimal trade-off that exists in-between security as well as resource utilization especially energy. The prime purpose of this paper is to develop a process of security in the context of wireless sensor networks (WSN) by introducing two types of sensor node deployed with different capabilities. The proposed algorithm Novel Model of Secure Paradigm (N-MSP) which is further integrated with WSN. However, this algorithm uses a Hash-based Message Authentication Code (HMAC) authentication followed by pairwise key establishment during data aggregation process in a WSN. The extensive simulation carried out in a numerical platform called MATLAB that depicts that the proposed N-MSP achieves optimal processing time along with energy efficient pairwise key establishment during data aggregation process.

Corresponding Author:

Manjunath B. E.,
Dept. of ECE,
Jain University,
Bangalore, India.
Email: manjunathbephd@gmail.com

1. INTRODUCTION

A WSN is formed with sensor nodes (SNs) using ad-hoc technology. Due to ad hoc technology, SNs are self-configured and operates the data transfer without any access points as well the computing takes place in a distributed manner. Traditionally, there exist many communication protocols such as Direct Communication (DC), Minimum transmission energy (MTE) protocol like hop-by-hop. The problem found in DC is the remote node from the sink die soon and is reserves in MTE, where nearby node die soon. A hierarchal routing mechanism, where the entire network is divided into groups called clusters, and a local sink in each cluster is elected which is called as a cluster head (CH) or aggregator node.

In initial cluster-based protocols, the cluster was static, which provides inconsistency of energy use because of the successive election of the same node as CH. The limitation of the static cluster is overcome in a state of artwork LEACH [1], wherein every communication cycle a new set of the cluster is formed and CH election. Since LEACH, enormous efforts are made by various other researchers towards developing new protocols for routing or communication, the collective information can be found in [2]. The WSNs having exploding usage into different critical applications since its conceptualization on the timeline, and the few to name includes (a) smart farming, (b) structural health monitoring, (c) fire detection in forest, (d) traffic congestion, etc. till Internet of Things (IoT) application so it is not just limited to military applications rather it has become a lifeline. The threats of attacks on this network are distinct philosophical to any network

security requirements. A detailed survey is about the current trend of a secure communication system in WSN is presented [3].

Although the most recent techniques to enhance the security paradigm in WSN networking environments are found efficient in securing the transmitted data packets still there exists a trade-off in between safety and energy consumption where most of the routing based and optimization based techniques lacks computational efficiency thus it generates power consumption overhead in overall systems. Therefore, by addressing this above stated issue the proposed study conceptualized an energy efficient framework namely N-MSP for secure data transmission and aggregation in a WSN.

The proposed secure framework adopted the features of Cryptography based security to authenticate the message to be transmitted through a wireless channel. The technique utilizes an HMAC based authentication scheme followed by pairwise key establishment during data aggregation process for two different type of node set up. However, an extensive simulation has been carried out to verify the performance efficiency of the proposed cryptography based N-MSP method which thereby depicts that being a light-weight security framework; it achieves very less computation time and energy consumption concerning iteration. It also shows that framework can easily manage the dynamicity of the network and performs the hash-based message authentication in the different parameterized scenario. The performance evaluation ensures its effectiveness on processing huge block size considering secure hash functions. The proposed framework also performs a secure data aggregation irrespective of any additional computing parameters. The paper organization is maintained as per the following orientation Section 2 describes all the significant conventional studies and their respective contributions where as Section 3 presents the conceptual system design for the prosed security paradigm, and Section 4 thereby discusses the implementation scenario, simulation results obtained and analysis, and finally Section 5 concerns to conclude the overall work.

2. REVIEW OF LITERATURE

The related work study can be broadly categorized into three groups namely (a) Techniques for Routing based security, (b) Techniques on Cryptographic-based security and (c) Techniques on Optimized security models.

2.1. Techniques for Routing based Security

Literature survey shows, the routing based security techniques normally implemented with the purpose of evolving security features on extensive routing operations. However, a closer look at the existing literature shows that most of the conventional routing strategies are considerably modified to some extent concerning security aspects. The prime objective of the existing studies was found more likely towards enhancing the security features of routing protocols.

The study of Das, et al.; [4] most recently introduced a WSN driven threat modeling system to bring resistance against wormhole as well as flooding attacks. Moreover, the study adopted the features of MAC scheme to ensure optimal security management in a WSN.

The study of Nandu and Shekokar [5] designed a conceptual model about the network authentication where the prime focus was laid towards defending DoS attack in WSN. The technique improvised the concept of re-programming along with the ease of decoding-encoding, selection of scope and versioning.

To address the critical factors of cloud-based security models, the study of Henze et al.; [6] presented a solution approach which involves confederation of IoT with cloud computing paradigm. The study ensures higher acceptance of the proposed vision into the real-time cloud-based applications by incorporating a comprehensive approach for privacy preservation of sensitive data. However, the method also enables the integrity of cloud services to enhance the adaptable interface for privacy requirements.

Sasikumar and Preetha [7] exhibited an extensive performance analysis of secure LEACH based clustering protocol from a theoretical perspective. However, most of the LEACH based protocols are found vulnerable to the security attacks. Keeping key design complexities of LEACH into the mind, the proposed study analyzes the performance competence of the secure-LEACH. The extensive simulation has been carried out considering the verification of every node's authenticity along with discarding bogus messages, intended to interrupt communication scenario. The outcome of the study thereby ensures the effectiveness of secure-LEACH in protecting the network from intruders.

The study of Flinn et al.; [8] introduced a unique application of A-Star algorithm using enhancing the heuristic component. The study is claimed to achieve a balanced flexibility in between the security and the network efficiency. The study outcomes are verified by different levels changing topologies which confirm that it ensures a high level of security at the cost of an optimal path when compared to the well-known Dijkstra's algorithm.

A ring based grouping mechanism for WSN has been introduced in the study of Mengyao et al.; [9].

The study mostly intended to perform a secure inter-cluster communication where the security features are mostly inclined towards supportable trust factors.

Adnan et al.; [10] conceptualized a secure protocol namely Secure Region-Based Geographic Routing Protocol (SRBGR) for WSN communication paradigm. The protocol has been designed with the aim of preventing undesirable packet transmission and increasing the probability of discovering relay nodes. The experimental outcomes demonstrate that SRBGR outperforms the conventional techniques n terms of packet delivery ratio. It also improves the network efficiency by resisting Sybil and blackhole attacks.

Masdari et al.; [11] tried to improve the performance efficiency of SECURE-LEACH protocol from all possible security aspects. Further, the extensibility is defined as per the standard protocol implementation scenario in WSN. The next segment discusses few of the significant contribution towards security enhancements for WSN using cryptographic-based techniques.

2.2. Techniques on Cryptography Based Security

Cryptography based authentication is another way to provide high-level security on network protocols. It incorporates encryption mechanism on transmitted data packets and makes it more secure while sending through wireless communication channels. It is more often provided secure communication by detecting vulnerable links on a WSN. However, most of the extensive reviews on cryptographic protocols exhibit the fact that the high-level conceptual design and respective implementation scenario of conventional cryptosystems are complex and error-prone. Thus it affects the performance of an overall system. However, the analysis says that either one can develop his cryptography technique or can modify the old ones. The most recent work carried out by Tomar et al.; [12] implemented an image-based authentication that enables ECC cryptography for secure key exchange. The design analysis of the algorithm shows that it utilizes very less key size and computing steps, thereby achieves computational efficiency regarding processing time and key exchange time. Experimental outcomes further display its effectiveness towards providing a secure layer to cloud computing networks.

The study of Soosahabi et al.; [13] presented a cryptographic probabilistic approach to the deliberately present state of transmission whether it could be a harmless or harmful state.

Kabir et al.; [14] formulated a security framework involving privacy preservation of sensitive and secret information. The proposed framework was claimed to be capable of handling security issues using symmetric key cryptography. The study simulates the proposed framework under parameterized and reconfigurable sensor nodes where execution time, memory, power consumption, and cost were considered as performance parameters. The findings of the proposed work were compared with the significant prior studies.

The study of Kodali and Sarma [15] an ECC based Diffe-Hellman key exchange protocol has been proposed and implemented. The outcome of the study was verified under extensive simulation and studied considering underlying protocol stack. The study outcomes offer lowered computational complexity during implementation.

2.3. Techniques for Optimized Security Models

The recent survey towards optimized security models for WSN paradigms has claimed it to be an active research area since 2010 onwards. In the recent past, most of the studies are found to adopt optimization models into their work such as the study of Narad and Chavan [16] incorporated the concept of the neural network to build up a new authentication scheme for WSN intensive routing operations.

Karapistol and Economides [17] have presented a modelling of security framework to address the jamming attack in WSN. The proposed system adhere the features of game theory and thereby simulated under extensive probability and utility factors. The design factors of the modelling considered the components of Stackelberg games. It can be seen in the study of [18] that same author has carried out an alternative simulation to detect the anomaly of respective events.

Poojashri et al.; [19] also introduced a game theoretical approach based framework to detect the node compromise attack in WSN. The proposed system namely intelligent Intruder Detection System (IDS) is proposed concerning three different functional components such as a combined framework using data fusion, neural network, and game theory. The obtained simulation results show that the proposed model can achieve significant outcomes while defending the attacks performed on sensitive information.

A bio-inspired algorithmic approach namely ant colony optimization has been utilized in the study of Alrajeh et al.; [20] where the outcomes were verified under several optimized performance parameters. The simulation results ensure its effectiveness in controlling data efficiency and minimizing the packet loss during transmission.

Another implementation of game theoretical approach can be found in the study of Ding et al.; [21] where the performance efficiency of the proposed model has been evaluated considering performance metric of energy consumption during ciphering, memory consumption and execution time.

TO tackle the issues of node attacks, a trust-based secure routing (TSR) mechanism is discussed in Ahmed et al. [22]. The outcomes of this mechanism under faulty node condition suggested that it achieves better delivery ratio and throughput. A review work towards the comparing the different asymmetric Cryptographic (ECC, RSA, DSA, etc.) algorithms was done for WNS by Singh and Chauhan [23] considering various parameters (weakness, key strength, attacks). The work introduced by Wang et al., [24] gives the security analysis for WSN by considering the wormhole attacks.With the designed security model author has achieved highly effective and accurate security for WSN.

3. SYSTEM MODEL OF N-MSP

The proposed system aims to formulate a novel framework to enhance the security parameters of conventional WSN considering a mix mode deployment strategy for two different types of sensor nodes such as TYPE-1 and TYPE-2 sensor nodes. However, the study also aims to achieve an optimal trade-off in between energy consumption and security during intensive routing operations. The following Figure 1 depicts the architectural framework of the conceptual model concerning key generation and clustering set up.

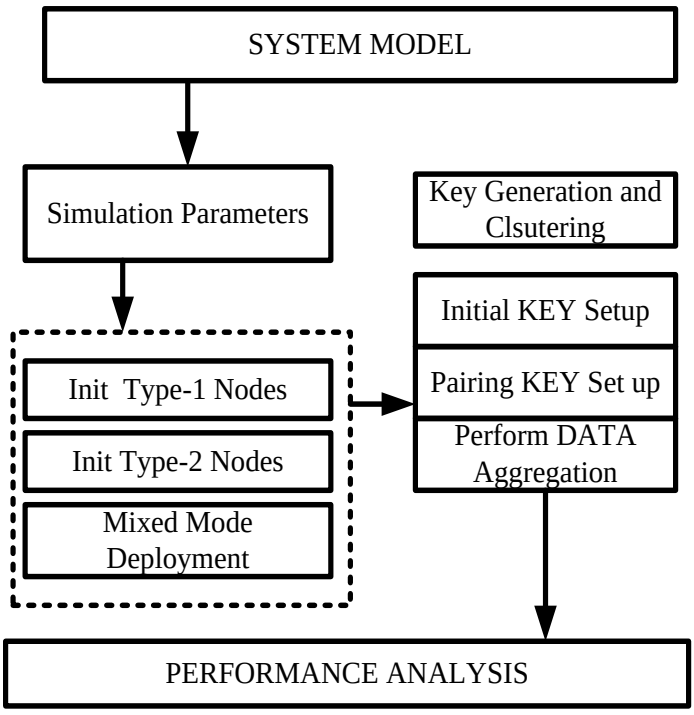

Figure 1. System Model of the Proposed Framework

The proposed system performs clustering of sensor nodes followed by secure data aggregation where the concept of Hash-based Message Authentication Code (HMAC) plays a significant role. The proposed model also uses a pairwise key generation process where each node generates unique key randomly with a combined entity of private and public key components. The framework thereby performs HMAC authentication scheme in each message transmitting from one sensor node to another during data aggregation process. The HMAC authentication initiates SHA-1, SHA-256,

SHA-384, SHA-512 based on the requirements to process block size of data. Finally, the obtained simulation results have been verified under several performance parameters regarding computation time T measurement concerning the number of iteration performed by the algorithm during pairwise key establishment and cluster key update. The experimental outcomes show the effectiveness of the proposed method for reducing the computational cost and energy overhead.

ALGORITHM ONE: *Proposed Energy-Efficient Secure Data Transmission in WSN*

Input: $N_{type1,}$ N_{type2}, A
Output: Secure DA and Energy Efficient Communication
START

1. Initialize N_{type1} , N_{type2} , A;
2. Generate *x, y* localization under boundary;
3. Generate coordinates of Type-1 nodes;
4. Generate coordinates of Type-2 nodes;
5. Perform mixed mode deployment;
6. Perform, Initial KEY Setup;
7. Init MP_{KEY}, PUB_{KEY}, Crypto(hash) ;
8. Concatenate MP_{KEY} , PUB_{KEY} , Crypto(hash) ;
9. PLOT N;
10. Formation of a cluster
11. Perform pairing KEY set up
12. Compute pair of $PAR_{P\text{-}KEY}$, $PAR_{PUB\text{-}KEY}$
13. Generate individual node key randomly
14. Perform HMAC, SHA-1 on N_{type1} data.
15. Perform pairwise KEY generation
16. FOR ($i \leftarrow 1: N_{type1}$)
17. **COMPUTE** Adv_{msg}
18. **COMPUTE** dist.
19. END
20. Connect N_{type1} with N_{type2}
21. Find out nodes within range
22. Set up communication
23. Select CH based on proximity
24. Select the node with minimum dist
25. Perform Data Aggregation

END

This algorithm depicts how the proposed N-MSP attains energy efficient securing data transmission by incorporating the concept of HMAC with pairwise key generation. However, in the initial step, the algorithm takes No. of Type-1 and Type-2 nodes as input and perform localization of respective nodes under a specific boundary (Line: 1-4). Further, the algorithm performs a mix mode deployment of these on a fixed area A with different types of capabilities (Line-5). The algorithm enables an initial KEY set up in every node to perform data encryption on their respective data (Line-6). Further, it also initiates MPKEY, PUBKEY and a Crypto(hash) to encrypt the data before transmission in the wireless network environment. Later on, it concatenates all the key values and forms the network parameters (Line: 7-10). However, the algorithm thereby formulates a clustering scheme for the ease of data aggregation and performs distribution of pairing KEY followed by computation of partial private and public key (Line:10-13). The framework incorporates a hash-based authentication scheme to validate every data packet which is present as follows with a mathematical expression (Line-14).

$$HMAC\ (MP_{KEY}, D) \leftarrow \quad (1)$$

$$H\ ((MP_{KEY}^{1} \otimes opad) \parallel H\ ((MP_{KEY}^{1} \otimes iPad) \parallel D)) \quad (2)\ [25]$$

The above Equation (2) exhibits that the Crypto (hash) performs outer padding and inner padding in MP_{KEY}^{1} before performing exclusive or and concatenation operation on the data D to be authenticated. The following Table 1 represents the symbols and their respective description used in Algorithm-1.

The algorithm further performs pairwise key generation and further precisely address the nodes which are within communication range. The cluster head selection is formulated based on a proximity orientation where the node resides within a minimum distance also taken into consideration. Finally, the algorithm performs the data aggregation before the initialization performance metrics. The next segment of the proposed study performs a simulation of the proposed N-MSP algorithm where the various performance metrics are taken into consideration to measure the computational efficiency of the proposed N-MSP to maintain a balance between security and energy consumption. The simulation has been carried out considering a numerical computing platform concerning different rounds.

Table 1. Symbol Representation

Sl. No	Symbol	Description
1	A	Deployment Area
2	N_{type1}	No of Sensor Node of Type-1
3	N_{type2}	No of Sensor Node of Type-2
4	*x*, *y*	Localization of Sensor Nodes
5	DA	Data Aggregation
6	MP_{KEY}	Master Private key
7	PUB_{KEY}	Public Key
8	Crypto(hash)	Cryptographic HASH function
9	N	Network parameter
10	Adv_{msg}	Advertisement Message
11	dist	Distance
12	$PAR_{P\text{-}KEY}$	Partial Private key
13	$PAR_{PUB\text{-}KEY}$	Partial Public key
14.	D	DATA
15	MP_{KEY}^{1}	Secret key derived from original key
16	H	Cryptographic Hash

4. SIMULATION ENVIRONMENT

The proposed algorithm namely N-MSP has been simulated under MATLAB Computing Platform running on 64-bit operating systems. The framework performs an extensive analysis of the proposed light-weight cryptography algorithm concerning several performance parameters.

The simulation studied to evaluate the processing time required during cluster key update which is plotted in (Figure 2), depicts that the proposed N-MSP achieves very less amount of processing time during encryption process with cluster key update concerning different level of iteration. Thereby, the asymptotic analysis conveys N-MSP's effectiveness on accomplishing computational efficiency. It also shows how the processing time of the proposed N-MSP has been computed considering the different velocity of mobile sensor nodes such as 1m/s, 2m/s, etc. However, in every simulation scenario more or less the proposed system achieves very less computation time.

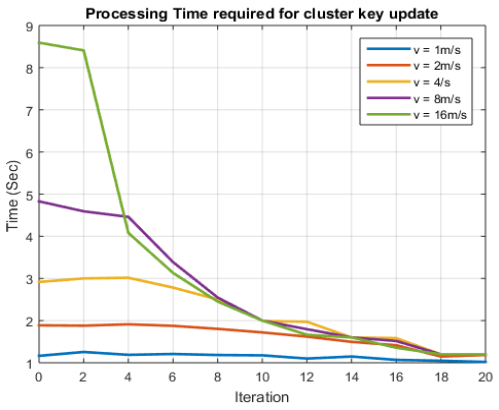

Figure 2. Iteration Vs. Processing Time (Sec)

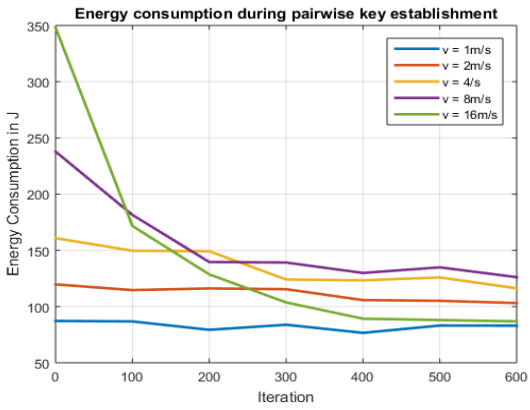

Figure 3. Iteration Vs. Energy Consumption (J)

The experimental outcomes also exhibit that despite having a capability to process a secure data transmission faster our proposed algorithm also archives an optimal trade-off in between the security and energy consumption. The extensive simulation carried out for observing the outcomes of pairwise key establishment steps reveals that the proposed N-MSP also consume very less amount of energy concerning iteration for different mobile nodes as in (Figure 3). The optimal energy consumption along with higher computational efficiency makes the algorithm extensible and more active in future research perspectives.

5. CONCLUSION

Secure data transmission in WSN has become one of the most active research areas for many years. The proposed study formulated a novel model of security paradigm namely N-MSP which can perform efficient, secure hash oriented message authentication in an energy efficient manner. The proposed technique

most adheres the features of HMAC based SHA-1 to authenticate every sensor messages before performing data aggregation on this. The obtained outcomes after simulating the proposed HMAC in a numerical computing simulation tool exhibits its effectiveness on achieving very less processing time and energy consumption. It also archives optimal trade-off in between energy and security. Moreover, the study ensures its extensibility in futuristic sensor applications.

REFERENCES

[1] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, *"Energy-efficient communication protocol for wireless microsensor networks,"* Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000, pp. 10. vol.2.

[2] M. Z. Hasan, H. Al-Rizzo; F. Al-Turjman, "A Survey on Multipath Routing Protocols for QoS Assurances in Real-Time Wireless Multimedia Sensor Networks," *in IEEE Communications Surveys & Tutorials*, No.99, pp.1-1, 2017.

[3] B.E. Manjunath and P.V. Rao, "Trends of Recent Secure Communication System and its Effectiveness in Wireless Sensor Network" *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol.7(9), pp131-139, 2016.

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

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

[6] M. Henze, "A comprehensive approach to privacy in the cloud-based Internet of Things," *Future Generation Computer Systems*, Vol. 56, pp.701-718, 2016.

[7] P. Sasikumar and K.S. Preetha, "Performance Analysis of Secure Leach Based Clustering Protocol in Wireless Sensor Networks," *International Journal of Applied Engineering Research*, Vol. 10(14), pp.34035-34041, 2015.

[8] J. Flinn, H. S. Choi Ortiz, and S. Yuan, *"A Secure Routing Scheme for Networks with Unknown or Dynamic Topology using A-star Algorithm,"* Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2016.

[9] 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.

[10] A.I. Adnan, Ali "A Secure Region-Based Geographic Routing Protocol (SRBGR) for Wireless Sensor Networks," *PloS one*, Vol. 12(1), 2017.

[11] 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*, Vol. 36(4), pp.1243-1260, 2013.

[12] A. S. Tomar, "Enhanced Image-Based Authentication with Secure Key Exchange Mechanism Using ECC in Cloud," *International Symposium on Security in Computing and Communication. Springer Singapore*, 2016.

[13] R. Soosahabi and M. N-Pour, "Scalable PHY-Layer Security for Distributed Detection in Wireless Sensor Network," *IEEE Transactions of Information Forensics and Security*, Vol. 7(4), pp. 1118-1126, 2012.

[14] A.F.M. Kabir, "Efficient and secured rekeying based key distribution in wireless sensor architecture with Arduino and XBee. Diss. Lethbridge, Alta.: The University of Lethbridge", *Dept. of Mathematics and Computer Science*, 2015.

[15] 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.

[16] 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.

[17] 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

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

[19] C.S.E. Poojashri, C. S., E. Sandeep Kumar, and S. V. Sathyanarayana. *"A game-theoretic approach for combating node compromise attack in Wireless Sensor Network,"* Communication and Signal Processing (ICCSP), International Conference, 2016.

[20] N.A. Alrajeh, M.S. Alabed, and M.S. Elwahiby, "Secure ant-based routing protocol for the wireless sensor network," *International Journal of Distributed Sensor Networks*, 2013.

[21] 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.

[22] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, "Countering Node Misbehavior Attacks Using Trust Based Secure Routing Protocol," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, Vol.13, No.1, pp. 260~268, March 2015.

[23] Pooja Singh, R.K. Chauhan, "A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN," *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 7, No. 4, pp. 2232~2240, August 2017.

[24] Hongbin Wang, Liping Feng, Rong Li, YiChi Zhang, "The Secure Localization Algorithm of SDV-HOP in Wireless Sensor Networks," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, Vol.14, No.3A, pp. 65~74, September 2016.

[25] H. Krawczyk, M. Bellare, R. Canetti,"HMAC: Keyed-Hashing for Message Authentication," *Network Working Group, Request for Comments*, 2014

BIOGRAPHIES OF AUTHORS

Manjunath B. E., pursuing Ph.D. under Jain University. I have completed my M.Tech from SSIT, Tumkur, VTU, Belagavi, Karnataka, India. My total work experience is around ten years. Attended a Three Day Workshop on "ROBOTRYST – 2013" in association with Tryst IIT-Delhi. Attended a Three Day National level Workshop on "Microcontroller MSP430 & its Applications" organized by HKBK College of Engineering, Bangalore in association with VTU, Belgaum, Karnataka State Council for Science and Technology, Bengaluru & M/s Advanced Electronics Systems at HKBK campus on 30th January to 1st February 2012. Participated in a five day Mission10x workshop on "Faculty Empowerment Program" conducted by Wipro, Bengaluru, from 23rd to 27th November 2009. Participated in a three day Mission10x Advanced workshop on "Faculty Empowerment Program" conducted by Wipro, Bengaluru. Participated in a one day workshop on " Recent Trends & Challenges in Indian Power Sector" organized by E&EE Dept., SKIT, Bengaluru, on 31st October 2009.

Dr. P.V. Rao., Professor, Dept. of E&C, I have completed Ph.D. at Dr. MGR University, Chennai in 2011. My total professional experience is around 23 years. My two Ph. D research scholars submitted a thesis and awaiting for final debate guiding five Ph. D candidates in the area of Low Power VLSI Signal processing and image processing from visvesvaraya Technical University, Belagavi, Karnataka, India.