Unique Analytical Modelling of Secure Communication in Wireless Sensor Network to Resist Maximum Threats

Manjunath B.E[1], Dr. P.V. Rao[2]
Research Scholar, Department of ECE, Jain University, Bangalore, India[1]
Professor, R&D Head, Department of ECE, VBIT, Hyderabad, India[2]

Abstract—**Security problems in Wireless Sensor Network (WSN) are still open-end problems. Qualitative evaluation of the existing approaches of security in WSN shows adoption of either complex cryptographic use or attack-specific solution. As WSN is an integral part of upcoming Internet-of-Things (IoT), the attack scenario becomes more complicated owing to the integration of two different forms of networks and so is for the attackers. Therefore, this paper introduces a novel secure communication technique that considers time, energy, and traffic environment as prominent constraints to perform security modeling. The proposed solution designed using analytical methodology has some unique capability to resist any form of illegitimate queries of network participation and yet maintain a superior form of communication service. The simulated outcome shows that the proposed system offers reduced end-to-end delay and highest energy retention as compared to other existing security approaches.**

Keywords—Encryption; energy; secure communication; threats; traffic environment; wireless sensor network

I. Introduction

Wireless Sensor Network (WSN) has been consistently being pivotal attention among the researchers owing to its capability to perform superior and cost-effective data transmission over the human non-accessible area [1][2]. It also has a wide range of application for various commercial monitoring and tracking services over various areas, e.g. healthcare, industrial, habitat, etc. [3]. However, irrespective of such an extensive list of application, there are various problems in WSN where researchers are still struggling to obtain end solution. There are various works of literature to prove that WSN still has unsolved problems associated with routing, energy, traffic management, security, energy, etc. [4][5]. A closer look into all these problems implicates that origination point of all the problems is associated with the sensor node which is characterized by low resource availability, low computational capability, as well as minimal memory/buffer. A typical MicaZ mote is characterized by 8-bit Atmel processor with 4KB of RAM and 512 KB of flash memory, which shows that it cannot with-held a very high-end communication requirement. Therefore, this area is always studied with respect to a group of nodes and not a single node. However, out of all the existing problems, security is undeniably the most potential issue to date. There is no denying the fact that cryptography has made significant progress with its wide range of applicability to various network systems [6]. However, it is unlikely that those cryptographic protocols even get installed in such miniature sensor node. For example, RSA (Rivest-Shamir Algorithm) is one of the most robust protocols known, but it cannot be executed over sensor node whose physical memory is 70% smaller than the size of the key of RSA [7]. At present, the solutions to offer security in the communication process in WSN is classified into two types: protocol-based and topology based [8]. The protocol-based techniques are more about the set of rules towards resisting specific attacks, e.g. security approaches based on multi-path based, negotiation-based, quality of service based, and query based.

Similarly, topology-based solution emphasizes on inducing security feature in the presence of different topologies, e.g. flat networking, hierarchical networking, and location-based networking. Key management is one of the most popular approaches to ensure implementation of potential encryption to address the complex problems of cryptographic protocols. However, some studies claim that not enough security solutions do exist for the upcoming and futuristic application of WSN. It is widely known now that WSN is the pathway to the Internet-of-Things that connects WSN with cloud [9]. Hence, the biggest set of challenges in such a network is to identify and resist threats existing in WSN and cloud. Existing security solutions are known to be very specific to attacks both for cloud as well as for WSN. Hence, the problem arises when it comes to identifying incoming attacks from the heterogeneous technological platform, and this fact calls for initiating an investigation without considering any specific attack model. A robust security model should offer a significant amount of resistance to the majority of the attackers, and more investigation should be encouraged in this direction. This fact is realized in proposed work where a dedicated attempt has been made to develop an encryption protocol that offers a significant level of security without predefining the attackers' type. The aim of the present work is also to ensure that a novel secure routing algorithm is formulated by hybridizing both topological-based approach and protocol-based approach. Section A discusses the existing literature towards secure communication in WSN using diversified security approaches and methodologies followed by a discussion of research problems that have been addressed in the present paper in Section B. The proposed solution towards resolving the security problems in WSN is discussed in C. Section II discusses algorithm implementation highlighting a discussion of four different forms of algorithm followed by a discussion of result analysis in Section III. Finally, the conclusive remarks are provided in Section IV.

A. Background

Exhaustive discussion about the prior approaches associated with secure transmission in WSN can be seen in our prior investigation [10]; this section further adds more information about recent works. The most recent work of Sen et al. [11] has discussed the relationship between communication security and energy factor with respect to the futuristic application of WSN. Jiang et al. [12] have presented a multi-factor authentication scheme using a key agreement protocol for securing the upcoming application of WSN. Ara et al. [13] have implemented a signature-based scheme for ensuring better privacy protection for resisting replay attacks mainly. Adoption of evidence-theory towards obtaining trust factor for securing communication in WSN is discussed in the work of Reddy et al. [14]. Usage of an identity-based encryption mechanism is seen in the work of Shim [15] that also targets to minimize computational and communication complexity associated with the authentication process in WSN. Key agreement protocol has been consistently claimed to offer better security even in case of mobility. Evidence of this fact was put forward by Al-Turjman et al. [16] where elliptical curve encryption and bilinear pairing is utilized. Study towards usage of composite ket Predistribution is another frequently used technique towards security in WSN. Study of Zhao [17] has proved that security features can be significantly enhanced using such technique. Shin and Kwon [18] have presented a novel authentication scheme towards any communication over WSN and 5G networks using a key agreement scheme. Huang et al. [19] have presented a solution towards privacy problems using enhanced homomorphic encryption mechanism. A unique methodology called as compression sensing was reported to offer secure networks as claimed in work presented by Dautov and Tsouri [20]. Privacy problems have also been addressed by He et al. [21] for resisting impersonation attacks using bilinear maps. Work of Hsu et al. [22] has presented secure group communication to maintain reduced communication cost in WSN. A similar direction of the study has also been continued by Porambage et al. [23]. Friesen et al. [24] have presented a secure prototype that integrates Bluetooth and WSN to offer secure communication in a vehicular network. Roy et al. [25] have presented a secure data fusion approach to identify the number of attackers present in the network. Lin and Wen [26] have discussed a technique that is meant for attack identification using clock synchronization scheme. Security towards dynamic networks can be ensured by using key management without any certificates. This fact has been claimed by the work of Seo et al. [27]. The work of Soosahabi et al. [28] has used probability theory to design their encryption scheme with lesser overhead. The work of Li [29] and Gu et al. [30] have used identity-based encryption and key pre-distribution scheme to restore maximum security in WSN. Therefore, there is multiple schemes towards secure communication in WSN with claimed advantages as well as unclaimed limitations overlooking various important criterion of security in WSN. The next section discusses such limitations that are highlighted in the form of research problem identification.

B. Research Problem

Significant research problems are as follows:

- Existing security approaches are highly specific to typical forms of attack scenarios which render inapplicable when the adversary is altered.
- Offering security by tracking time-based behavior is something that is utterly missing in existing approaches.
- Existing usage of cryptographic protocols offers significant security but at the cost of multiple resource dependencies for the resource-constraint nodes.
- Maintaining equilibrium between dynamic traffic condition and superior resistivity to an unknown form of attacks is still an open challenge in secure communication in WSN.

Therefore, the problem statement of the proposed study can be stated as "Developing a comprehensive algorithm that emphasizes on superior security as well as optimal communication performance with good control over computational complexity in WSN is still unsolved."

C. Proposed Solution

The proposed work is a continuation of our prior work [31] where an authentication policy has been presented using the establishment of pairwise keys in WSN. Although this model offers secure authentication, less emphasis was offered on traffic dynamics and resource dependencies. This gap is fulfilled in the proposed study where a proposed model is presented with a primary intention of offering secure communication using a lightweight encryption policy. The model also targets to maintain a better equilibrium between traffic dynamics and resource decencies to prove the practicality of implementing a secure routing protocol. The proposed system adopts an analytical research methodology to implement this concept. The schematic diagram of the proposed model is highlighted in Fig. 1.

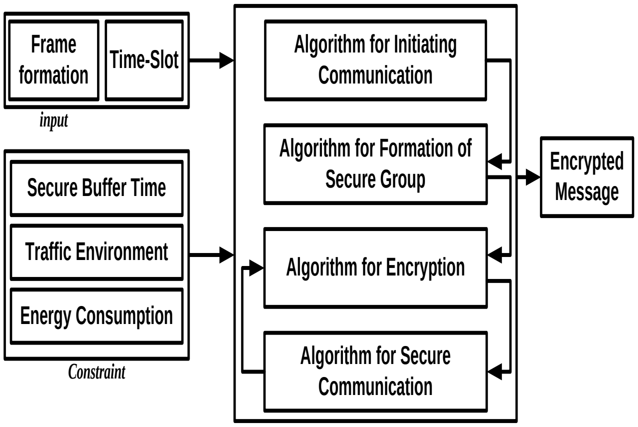

Fig. 1. Proposed Schema of Secure Communication in WSN.

According to the schematic diagram, there are three essential blocks, i.e. input block, constraint block, and algorithm block. The input block is all about framing control message and data required for communication. The time-slot is used for capturing every record of routing events especially during route request, route response, route acknowledgment, and node syncing process. This assists in tracking all the time-based records used for understanding the routes as well as shaping the security feature as well. The constraint block consists of secure buffer time where is the time duration between two control messages to be exchanged among each other while performing secure routing. The traffic environment block is responsible for replicating the actual traffic behavior in WSN while energy consumption block is about estimating the amount of energy being allocated as well as being drained while performing secure data aggregation process. The final block is all about different set of algorithms that performs multiple tasks e.g. performing preliminary communication among the nodes using control message, formation of group-based communication system from all the nodes to the base station, implementing a novel and straightforward encryption algorithm for ciphering the control being routed, and finally ensuring the ciphering of the data being forwarded to the base station. The complete process leads to the generation of an encrypted data which if falls in the wrong hand, i.e., malicious node will be of no use for them as there are multiple complex dependencies to perform decryption and thereby it significantly discourages any attackers either to initiate or to continue their malicious activity. The next section elaborates about algorithm implementation.

II. Algorithm Implementation

The algorithm mainly emphasizes on introduces smart and lightweight encryption in WSN such that it could maintain a good balance between superior security features with higher resource saving at the same time. The initial stage of the algorithm initializes the network parameters, e.g., defining the number of the sensor node and positioning the base station to initiate the simulation area. The algorithm also introduces a novel logic of security buffer time which is a gap of time difference while forwarding secure control messages followed by choosing an encryption mechanism. The first algorithm is responsible for initiating preliminary communication among the nodes by taking the input of n (number of sensors), b (base station), b_t (security buffer time), and s_d (spatial distance) that after processing yields an outcome of the *link* (generated link). The significant steps of the proposed algorithm are as follows:

```
Algorithm for Initiating Communication
Input: $n, b, b_t, s_d$
Output: link
Start
1. init $n, b, b_t$,
2.  For $i$=1: n
3.   If $s_d<s_r$
4.     $R_{mat}$[(i, n+1) (n+1, i)]=1
5.   End
6.  For $j$=1: $n$
7.     [link]→$f_1(R_{mat}, \alpha)$
8.  End
End
```

The description of the above algorithm steps is: The algorithm first initializes all the input parameters (Line-1) and constructs a spatial matrix S_{mat} by considering the pairwise distance among all the sensor nodes. It means that all the node's locations in the form of S_{mat} are now known to all the sensors as well as base station too. The advantage is that if there is any other node attempting to initiate a communication process their existence will not present in S_{mat} and hence all possible communication will be aborted in this initial security check itself. For all the sensor nodes (Line-2), the algorithm checks if the distance between the node and base station, i.e. s_d is lesser than sensing range, i.e. s_r (Line-3). In this case, the algorithm constructs a matrix of storing routing information called as R_{mat} (Line-4). It is assumed that the matrix R_{mat} will reposit only those matrix elements of S_{mat} which are found lesser than or equal to sensing range (i.e., $S_{mat} \leq s_r$). A new two-dimensional matrix α is constructed which will reposit information related to recent communication nodes and the base station. This advantage is that it will retain records of all the node-base communication in the different matrix so that if any of the nodes gets compromised. This information related to routing is safely maintained within the base station. Hence, this is the second layer of security that offers a validation check for all communicating sensors. Finally, the algorithm constructs links between two communicating nodes by applying a function $f_1(x)$ over routing matrix R_{mat} and two-dimensional matrix α (Line-7). The construction of $f_1(x)$ as routing scheme is designed using graph theory by exploring the entire shortest route from all the vertices to the sink node (this routing will exactly mimic the data aggregation process). However, such forms of communications happen in node level and may possible leads to overhead for a long run even though it maintains two layers of checks for the validation of a participating sensor. This problem is mitigating by grouping the sensors and then performing communication.

The algorithm for grouping takes the input of s_g (secure group) that after processing yields and outcome of *sg_ind* (secure group index). The descriptions of algorithmic steps are as follows: The algorithm should take the input of the number of secure groups (Line-1). A unique form of grouping is carried out in this part which calls for obtaining both single and multiple secure links. For the entire sensor (Line-2), a matrix for the secure link is constructed (Line-3) followed by repositing all the single links in that matrix initially. The computation further narrows down only to the number of secure groups (Line-5); it checks if the counter value is less than ns_g (Line-6). Under this condition, it will mean that all the assigned number of secure groups will be needed to be considered which address the problems if any one of the group will misbehave by not participating in the data aggregation process. A function $f_2(x)$ is constructed by arbitrarily permuting the number of sensors, and this function chooses constant c and another function $g(n)$, where constant c is calculated as the rounded value of (j-1), and function $g(n)$ is equivalent to n divided by ns_g (Line-7). This results in indexing of all secure groups *sg_ind* (Line-12). The steps included in this algorithm are as follows

Algorithm for Formation of Secure Group

```
Input: $s_g$
Output: $sg\_ind$
Start
1. init $s_g$,
2. For i=1:n
3.    obtain secLink
4. End
5. For j=1: $ns_g$
6.   If j<$ns_g$
7.     ind→$f_2$(c.$g$(n)+1:j.g(n))
8.   Else
9.     $ind$→$f_2$($c.g$(n))
10.End
12.  $sg\_ind$→$j$
End
```

The complete execution of the above-mentioned algorithm will result in secure formation and identification of all the groups that are secured, and this is now followed by forwarding a secure message further for secure synching all the security groups. For this process, the algorithm will attempt to find all the index of secure groups that match with the time slots of nodes. This is an interesting fact where each communicating nodes will all have similar time-slots which will never match with any new node (which could be malicious node/selfish node too). This will lead to the forwarding of the secure sync message only to the legitimate nodes and never to any unregistered/malicious nodes. Hence, algorithm-1 and algorithm-2 apply the non-cryptographic mechanism to initiate security measures; however, for effective security there is a need for encryption protocol. This objective is fulfilled by the third algorithm that offers an extremely lightweight algorithm to perform encryption. This algorithm takes the input of *msg* (message) that after processing will lead to the generation of *encMsg* (secure message). The steps included in this algorithm are:

Algorithm for Encryption

```
Input: $msg$
Output: $encMsg$
Start
1. init $m$
2. $msg$→$\theta_1$($msg$)
3. $msg$→$msg^T$
4. For $i$=1:64: size($msg$)
5.    [encMsg, $s_{key}$]=$f_3$($msg$, $s_{key}$)
6. End
End
```

The proposed system applies simple steps for performing encryption. The function developed for this purpose takes the input of message (Line-1), and its output arguments are encrypted data along with the secure key of 64 bits. The first task of this encryption algorithm is to apply an increase the precision of the matrix storing the message in double form, which is followed by further application of simple encryption function θ_1 that is capable of converting the decimal value to the binary value (Line-2). A further transposition of the message matrix is carried out (Line-3). A loop is constructed that starts from 1 and ends up at the size of the message with a difference of 64 bits (Line-4). This operation is further followed by applying a function $f_3(x)$ on the message and secure key s_{key} (Line-5). From the encryption operation viewpoint, it can be said that this algorithm offers simple and lightweight encryption as it takes the input of 64-bit message with either 56 bit or 64 bit as the maximum size of the key to generate an encrypted message of 64-bit. There is good flexibility in allocating the memory of this secure key. In case the memory allocation is of 64 bits than the algorithm will be bound to check for its bit parities but if the size is reduced to 56-bits than the algorithm will involuntarily add 8-bits as a parity check. Interestingly, the proposed system will not utilize this extra 8 bits in either encryption or decryption process. Hence, if there is a man in middle attack compromise this keys, they will attempt to use this extra 8-bit parity which will lead to a generation of a different key that will never match with the generated secure key. Hence, a robust and lightweight encryption algorithm is presented in the proposed system. The significant advantage of this encryption algorithm is that it offers significant control over the size of the message as well as secret key and hence it allows significant flexibility to the WSN to operate even in a large scale deployment.

Although, the above-mentioned security algorithm assists in encryption, it is required to be discussed the exact procedure to perform secure communication. The algorithm to carry out secure communication takes the input of AP (active period), s_{frm} (size of frame), b_t (Secure buffer time), and β (percentage of message urgency) that after processing leads to the generation of data (secure data forwarding). The steps included in the proposed algorithm are as follows:

Algorithm for Secure Communication

```
Input: $AP$, $s_{frm}$, $b_t$, $\beta$
Output: $data$
Start
1. $init$ AP, $s_{frm}$, $b_t$, $\beta$
2. CAT→explore($B_{rate}$)
3. nβ→$f_3$(size(CAT)* β/100)
4. Apply Algorithm for encryption
5. For i+1:n        //Line-752
6.   h→$\arg_{min}\{E_{TX}$→$f_4$(d, data)}
7. End
8. Forward data
End
```

This part of the algorithm implementation considers various metric associated with the time of specific operation in WSN. The algorithm computes both duration of awake as well as sleep considering the active period and size of the frame. These time-based parameters are utilized for computing time required for each event in WSN viz. time for performing synching, time for forwarding route response, sleep time for data communication, and time of forwarding route acknowledgment. After initialization (Line-1), the algorithm computes buffer rate B_{rate} with respect to the number of time slots used. The next step will be to construct a matrix CAT, i.e. Connection Arrival Time for exploring the exact B_{rate} (Line-2) followed by computation of node identity and defining a variable β for specifying urgency of the message to be transmitted. A new function $f_3(x)$ is defined that can compute the number of such urgent message mathematical expression shown in Line-3. Further, the encryption algorithm is implemented so that it can secure all the messages being exchanged among the nodes. This encryption algorithm will be now suitably modified to ensure that it secures data as well. For that purpose, the algorithm considers all the communication nodes n (Line-5) with initialization of message size and data packets. It is followed by the computation of transmittance energy E_{TX} using function f_4(x) on the distance between all communicating nodes and data (Line-6). The proposed system constructs the function $f_4(x)$ using first order- radio-energy model. The construction of this $f_4(x)$ is as follows: Different energy-related variables, e.g. transmittance energy, amplification energy, receiving energy, size of data packets, and distance is initialized first. Then a condition is constructed which checks that if the distance between two communicating nodes is more than a threshold distance than total energy consumption is calculated as the fourth power of same distance along with consideration of E_{TX}, data, and amplified energy or else square of the distance is considered. This is a greedy-approach, which will always look for lower power consumption, i.e. where the E_{TX} can be computed as squared of distance. Therefore, the proposed algorithm always ensures that there is a good balance between energy consumption and security feature. Finally, the algorithm forwards its data in the most secure manner as well as it also restores a significant amount of computational resources in WSN. The next section discusses the outcomes obtained from implementing the proposed algorithm.

III. Result Analysis

As the prominent aim of the proposed research work is to offer a robust, secure communication scheme by balancing both security requirements as well as communication requirements, the analysis of the proposed framework is carried out using three essential parameters, i.e. delay and energy factor. Computation of delay will offer the insights of the capability of the proposed framework to offer faster establishment of secure routing while computation of energy will offer insight about the practicality of using this protocol in the resource-constrained sensor node. Implemented on MATLAB, the study is assessed using 100-1000 sensor nodes in the presence of 1-10 seconds of secure buffer time. Analysis with respect to secure buffer time is essential as it is required to check the influence of increasing buffer time on communication performance. The outcome of the proposed study has been compared with two related frameworks called as SEEM and FlexiCast that has been introduced by Naseer [32] and Lee [33]. They are found to be frequently referred bby research community to address security problems in WSN, and hence they are considered in present analysis too.

Fig. 3 highlights that proposed system (ProP) offers reduced delay as compared to SEEM and Flexicast protocol. The approach of SEEM has an increasing number of steps to perform route maintenance at the end stage that consumes a considerable amount of time leading to increased delay compared to the proposed system. Moreover, usage of FlexiCast calls for iterative steps of using Bloom Filters along with generation of fingerprints that are required to be validated twice. Therefore, irrespective of the fact that FlexiCast offers better security than SEEM, it still consumes more time leading to delay slightly higher than SEEM.

A closer look into Fig. 2 highlights that performance of the proposed system as well as FlexiCast is nearly the same and has proven the higher amount of residual energy while SEEM doesn't seem to offer better retention of energy. However, after an in-depth investigation, it was found that the proposed system offers slightly better retention capability of energy as compared to FlexiCast. The prime reason behind this is proposed system offers usage of mainly lightweight cryptography where the size of keys can be controlled in each increasing rounds of secure buffer time. This causes less consumption of energy over the long run, and hence the curve of energy remains more-or-less the same with less fluctuation. Hence, network lifetime can be ensured for the proposed system. However, SEEM approach includes quite a complex and iterative search procedure for establishing new secure links resulting in degradation of remnant energy.

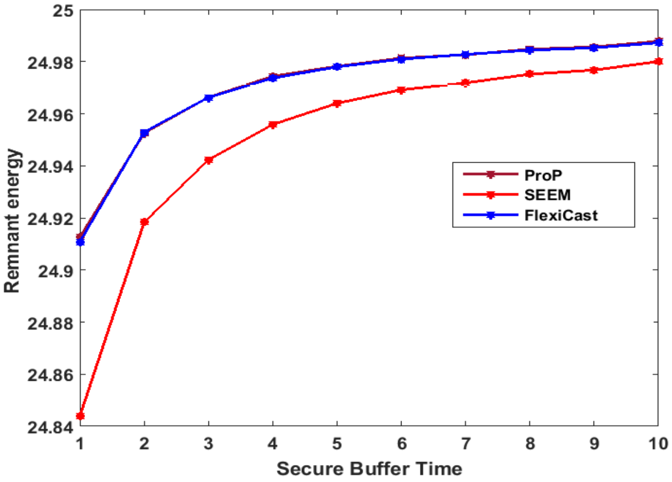

Fig. 2. Comparative Analysis of Remnant Energy.

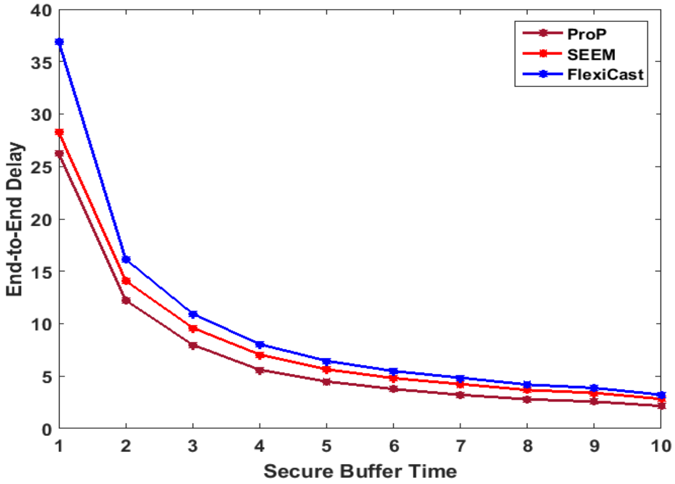

Fig. 3. Comparative Analysis of End-To-End Delay.

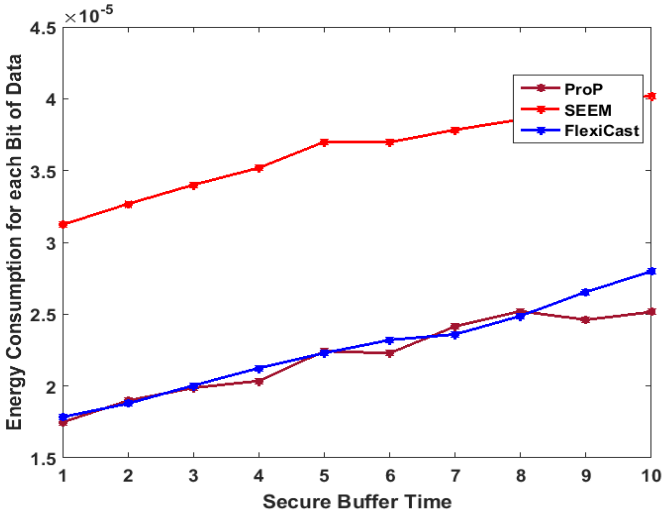

Fig. 4. Comparative Analysis of Energy Consumption.

Fig. 4 highlights similar energy performance of all the considered approach. The performance of the proposed system has always been found to minimize energy consumption with the increase of secure buffer time. This fact will mean that proposed system retains the capability to identify traffic behavior and it then suitably balances the security performance with its message transmission performance. The FlexiCast mechanism also involves hashing operation along with usage of increasing components of authentication using bloom filters, which causes increased dependency of resources to perform encryption with a variable rate of traffic. Hence, it cannot retain maximum energy retention for a more extended period, and soon it drains out. A similar fact is also applicable for SEEM approach too. Hence, energy consumption for the proposed system is found to be better than FlexiCast for the long run over secure buffer time.

IV. Conclusion

This paper brief of a novel and straightforward security-based solution to resists majority of the lethal threats over WSN. The significant contributions of this paper are viz. i) the model consider three different forms of non-linear constraints, e.g. time, traffic situation, and energy, which can't be seen in any existing security approaches in WSN; ii) the encryption mechanism doesn't have any form of iterations or recursive steps which makes the model very lightweight unlike any existing cryptographic models in WSN; iii) the model can be said to be a hybridized form of topological-based and protocol-based security approach and hence its resistivity towards different attacks are quite high compared to other techniques; iv) this model reports of using time factor against all forms of operations during route discovery in order to facilitate identification of malicious node very easily. At present, there are various models to detect malicious behavior, but very few of them has been reported to consider such time-factors of recording route discovery messages; v) the proposed technique offers a significant scale of security towards control message and then to data package because of this the attackers are completely unaware of even identifying the formation of the message and data contents in the packet. Most importantly, the study outcome has exhibited that the proposed technique has offered better communication performance in contrast to existing approaches to secure communication in WSN. This proves that the proposed model can be well adopted in practical implementation scenario with its response time 90% faster as compared to any other security algorithms.

The proposed model can be adapted in future to enhance further security level by adapting different security algorithms and reduce the risk of threats.

References

[1] Dac-Nhuong Le, Raghvenda Kumar, Jyotir Moy Chetterjee, Introductory Concepts of Wireless Sensor Network. Theory and Applications, GRIN Verlag, 2018

[2] Fadi Al-Turjman, Wireless Sensor Networks: Deployment Strategies for Outdoor Monitoring, CRC Press, 2018

[3] Kamila, Narendra Kumar, Handbook of Research on Wireless Sensor Network Trends, Technologies, and Applications, IGI Global, 2016

[4] V. P. Bawage and D. C. Mehetre, "Energy efficient Secured Routing model for wireless sensor networks," 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, 2016, pp. 865-869.

[5] S. Pourazarm and C. G. Cassandras, "Energy-Based Lifetime Maximization and Security of Wireless-Sensor Networks With General Nonideal Battery Models," in IEEE Transactions on Control of Network Systems, vol. 4, no. 2, pp. 323-335, June 2017.

[6] W. Julian Okello, Q. Liu, F. Ali Siddiqui and C. Zhang, "A survey of the current state of lightweight cryptography for the Internet of things," 2017 International Conference on Computer, Information and Telecommunication Systems (CITS), Dalian, 2017, pp. 292-296.

[7] Balasubramanian, Kannan, Rajakani, M., Algorithmic Strategies for Solving Complex Problems in Cryptography, IGI Global, 2017

[8] Smain Femmam, Building Wireless Sensor Networks: Application to Routing and Data Diffusion, Elsevier, 2017

[9] Dawson, Maurice, Eltayeb, Mohamed, Omar, Marwan, Security Solutions for Hyperconnectivity and the Internet of Things, IGI Global, 2016

[10] Manjunath B E, P.V. Rao, " Trends of Recent Secure Communication System and its Effectiveness in Wireless Sensor Network", International Journal of Advanced Computer Science and Applications, Vol. 7, No. 9, 2016

[11] S.Sen, J.Koo, S.Bagchi, "TRIFECTA: Security, Energy Efficiency, and Communication Capacity Comparison for Wireless IoT Devices", IEEE Internet Computing, 2018

[12] Q. Jiang, S. Zeadally, J. Ma and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," in *IEEE Access*, vol. 5, pp. 3376-3392, 2017.

[13] A. Ara, M. Al-Rodhaan, Y. Tian and A. Al-Dhelaan, "A Secure Privacy-Preserving Data Aggregation Scheme Based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems," in *IEEE Access*, vol. 5, pp. 12601-12617, 2017.

[14] V. Busi Reddy, S. Venkataraman and A. Negi, "Communication and Data Trust for Wireless Sensor Networks Using D–S Theory," in *IEEE Sensors Journal*, vol. 17, no. 12, pp. 3921-3929, June15, 15 2017.

[15] K. A. Shim, "BASIS: A Practical Multi-User Broadcast Authentication Scheme in Wireless Sensor Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1545-1554, July 2017.

[16] F. Al-Turjman, Y. Kirsal Ever, E. Ever, H. X. Nguyen and D. B. David, "Seamless Key Agreement Framework for Mobile-Sink in IoT Based Cloud-Centric Secured Public Safety Sensor Networks," in *IEEE Access*, vol. 5, pp. 24617-24631, 2017.

[17] J. Zhao, "Topological Properties of Secure Wireless Sensor Networks Under the q -Composite Key Predistribution Scheme With Unreliable Links," in IEEE/ACM Transactions on Networking, vol. 25, no. 3, pp. 1789-1802, June 2017.

[18] S. Shin and T. Kwon, "Two-Factor Authenticated Key Agreement Supporting Unlinkability in 5G-Integrated Wireless Sensor Networks," in IEEE Access, vol. 6, pp. 11229-11241, 2018.

[19] H. Huang, T. Gong, P. Chen, R. Malekian and T. Chen, "Secure two-party distance computation protocol based on privacy homomorphism and scalar product in wireless sensor networks," in Tsinghua Science and Technology, vol. 21, no. 4, pp. 385-396, Aug. 2016.

[20] R. Dautov and G. R. Tsouri, "Securing While Sampling in Wireless Body Area Networks With Application to Electrocardiography," in IEEE Journal of Biomedical and Health Informatics, vol. 20, no. 1, pp. 135-142, Jan. 2016.

[21] D. He, S. Zeadally, N. Kumar and J. H. Lee, "Anonymous Authentication for Wireless Body Area Networks With Provable Security," in IEEE Systems Journal, vol. 11, no. 4, pp. 2590-2601, Dec. 2017.

[22] C. F. Hsu, L. Harn, T. He and M. Zhang, "Efficient Group Key Transfer Protocol for WSNs," in IEEE Sensors Journal, vol. 16, no. 11, pp. 4515-4520, June1, 2016.

[23] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila and B. Stiller, "Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications," in IEEE Access, vol. 3, pp. 1503-1511, 2015.

[24] M. Friesen, R. Jacob, P. Grestoni, T. Mailey, M. R. Friesen and R. D. McLeod, "Vehicular Traffic Monitoring Using Bluetooth Scanning Over a Wireless Sensor Network," in Canadian Journal of Electrical and Computer Engineering, vol. 37, no. 3, pp. 135-144, Summer 2014.

[25] S. Roy, M. Conti, S. Setia and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 681-694, April 2014.

[26] S. C. Lin and C. Y. Wen, "Device-Based Asynchronous Ranging and Node Identification for Wireless Sensor Networks," in IEEE Sensors Journal, vol. 14, no. 10, pp. 3648-3661, Oct. 2014.

[27] S. H. Seo, J. Won, S. Sultana and E. Bertino, "Effective Key Management in Dynamic Wireless Sensor Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 371-383, Feb. 2015.

[28] R. Soosahabi, M. Naraghi-Pour, D. Perkins and M. A. Bayoumi, "Optimal Probabilistic Encryption for Secure Detection in Wireless Sensor Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 375-385, March 2014.

[29] F. Li and P. Xiong, "Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things," in *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3677-3684, Oct. 2013.

[30] W. Gu, N. Dutta, S. Chellappan and X. Bai, "Providing End-to-End Secure Communications in Wireless Sensor Networks," in *IEEE Transactions on Network and Service Management*, vol. 8, no. 3, pp. 205-218, September 2011.

[31] Manjunath B E, P.V. Rao, " Balancing Trade-off between Data Security and Energy Model for Wireless Sensor Network", International Journal of Electrical and Computer Engineering, Vol. 8, No. 2, April 2018, pp. 1048~1055

[32] N.Nasser , Y. Chen, "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks", Elsevier, Vol. 30, pp. 2401-2412, 2007

[33] J. Lee, L. Kim and T. Kwon, "FlexiCast: Energy-Efficient Software Integrity Checks to Build Secure Industrial Wireless Active Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 6-14, Feb. 2016.