Efficient Random Key based Encryption System for Data Packet Confidentiality in WSNs

Kashif Saleem,
Mohammed Sayim Khalil
Center of Excellence in Information Assurance (CoEIA)
King Saud University (KSU)
Riyadh, Saudi Arabia
{ksaleem, sayimkhalil}@ksu.edu.sa

Norsheila Fisal,
Adel Ali Ahmed
Telematic Research Group (TRG),
Faculty of Electrical Engineering (FKE)
Universiti Teknologi Malaysia
Skudai, Malaysia
sheila@fke.utm.my

Mehmet A. Orgun
Department of Computing
Macquarie University
NSW 2109, Australia
mehmet@science.mq.edu.au

***Abstract*—Wireless sensor networks (WSNs) consists of numerous tiny wireless sensor nodes to communicate with each other with limited resources. The resource limitations and vulnerabilities of wireless sensor node expose the network to suffer with numerous attacks. The WSN constraints and limitations should be taken under consideration while designing the security mechanism. The recent Biological inspired self-organized secure autonomous routing protocol (BIOSARP) requires certain amount of time at initialization phase of WSN deployment to develop overall network knowledge. Initialization phase is a critical stage in the overall life span of WSN that requires an efficient active security measures. Therefore, in this paper we propose E-BIOSARP that enhances the BIOSARP with random key encryption and decryption mechanism. We present the design, pseudo code and the simulation results to prove the efficiency of E-BIOSARP for WSN. Network simulator 2 (NS2) has been utilized to perform the analysis. Our result shows that proposed E-BIOSARP can efficiently protect WSN from spoofed, altered or replayed routing information attacks, selective forwarding, acknowledgement spoofing, sybil attack and hello flood attack.**

***Keywords*—Authentication, Decryption, Encryption, Human Immune Blood Brain Barrier, Malicious, Multihop, Random Key, Routing, Secure, Wireless Sensor Network**

I. INTRODUCTION

Wireless communication plays an important role these days in the sector of telecommunication and has huge importance for future research. There has been an exponential growth in wireless communication due to the development of different devices and applications. Researchers recently develop a new approach in wireless system design: one that involves low-cost embedded devices that can be implemented for a variety of applications [1]. These small and low cost sensor nodes became technically and economically feasible [2]. The sensor node is a miniaturized device as shown in Figure 1, equipped with sensors like temperature, humidity, light, sound, etc. Nevertheless, due to the extremely small architecture, the sensors lacks in storage space, energy supply and communication width. For example, a sensor typically has 8-120KB of code memory and 512-4096 bytes of data memory. The transmission bandwidth ranges from 10kbps to 115kbps. The sensor nodes are programmed to work in a self-organized way. Due to their autonomous capability, the sensor nodes can transfer the sensed data node by node to the destination known as base station (BS). In some cases base station is called as sink node. The amount of base stations (like laptop, PDA, gateway to other networks, etc) in the deployed network depends on the application requirements. Enormous numbers of these disposable sensor nodes come up with a wireless sensor network (WSN) as shown in Figure 2.

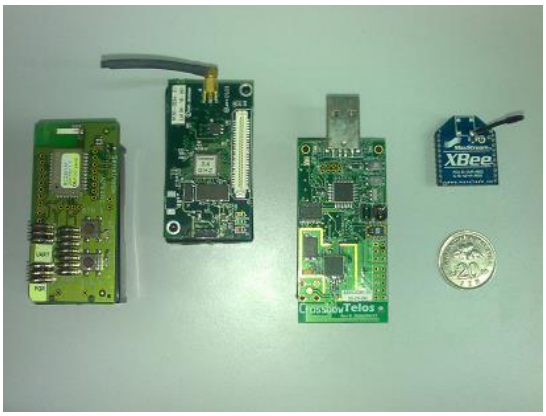


Figure 1. Wireless Sensor Nodes [3]

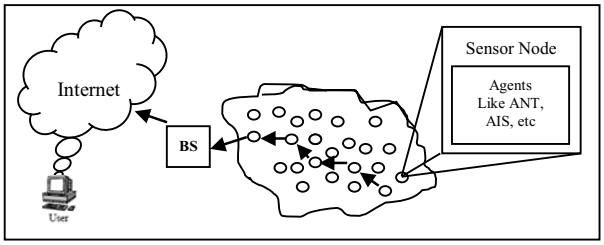


Figure 2. Wireless Sensor Network [3]

978-0-7695-5022-0/13 $26.00 © 2013 IEEE
DOI 10.1109/TrustCom.2013.206

The routing strategies and WSN modeling are getting much preference; the security issues do not receive extensive focus. In WSNs, many routing protocols are very simple, and for this reason WSN is sensitive to attacks. In WSN, an adversary can either deploy his own node or compromise some nodes. The compromised node can take many actions to create a network layer attacks. Attacks depend on manipulated sensor data are divided into two classes: first are the attacks that try to manipulate user data directly and the other try to affect the underlying routing topology.

It is imperative that the security concerns be addressed from the beginning of the system design [4]. Because of resource limitation and vulnerabilities of wireless communication, it is easier to suffer all kinds of attacks, if the wireless sensor nodes are deployed in the environment that is unprotected/hostile. These attacks involve signal jamming and eavesdropping, tempering, spoofing, resource exhaustion, altered or replayed routing information, selective forwarding, sinkhole attacks, Sybil attacks, wormhole attacks, flooding attacks and so on [5, 6]. Many papers proposed the countermeasures of these attacks and the majority of these are based on encryption and authentication.

In [7] the authors have come up with Bio-inspired autonomous routing protocol (BIOARP) that utilizes ANT Colony Optimization (ACO) for the optimum route discovery in WSN. Additionally, in [3] the authors have enhanced BIOlogical Inspired Self-organized Secure Autonomous Routing Protocol (BIOSARP) with self-security management module on top of BIOARP that depends on artificial immune system (AIS). The BIOSARP method is based on the behavior of human immune system (HIS). The major aspect of HIS is to detect the anomalies by differentiating between self and non-self entities. The HIS security is used in the computer world with the name of artificial immune system (AIS).

In this paper, we proposed E-BIOSARP that enhances BIOSARP with random key encryption and decryption mechanism, similar to human immune blood brain barrier (BBB) system [8, 9]. With the help of encryption mechanism, WSN communication is secure even in the phase of initialization. Furthermore, the design, pseudo code and the detailed simulation results are exposed to prove the accuracy of random key encryption and decryption mechanism for WSN.

Next section elaborates the most related and recent literature review. Section 2 describes the architecture of E-BIOSARP random key encryption and decryption mechanism. Section 3 shows the implementation and results. The conclusion and future work are discussed in section 4.

II. RELATED WORK

Owing to the factor of initialization phase, the WSN need security mechanism to be in operation before the network deployment means in initialization phase. As stated in [10] node cloning attacks can be mounted only during deployment since a cloned node cannot initiate the protocol with success; it can be successfully connected only by acting as a responding node. Recent progress in implementation of elliptic curve cryptography (ECC) on sensors proves public key cryptography (PKC) is now feasible for resource constrained sensors [11]. Given the efficient low-layer primitive in place, the high-layer PKC based security scheme design in sensor networks, however, is not straightforward due to the special hardware characteristics and requirements of WSNs. Therefore, the performance of PKC based security schemes is still not well investigated.

The mechanism pairwise key establishment (PKE) based on transitory master keys as discussed in [10] is particularly useful for the purpose. LEAP++ consists of system setup, pairwise key establishment and authentication key disclosure. Given mechanism wants large enough time and resources in generating pre-authenticators before deployment. Security in natural inspired routing protocols is still an open issue. Widespread acceptance and adoption of these protocols in real world wireless networks would not be possible until their security aspects have thoroughly been investigated. Authors have showed that the energy consume on sending and receiving packet is much less.

In [12], the authors have presented suite of security protocols optimized for sensor networks (SPINS). SPINS algorithm is actually the enhancement and merging of two security algorithm Secure Network Encryption Protocol (SNEP) and micro version of TESLA (µTESLA). Mainly the problem tackled by the authors is the complexity of security algorithm specifically for low cost miniaturized sensor nodes. Already, SNEP and µTESLA provides data confidentiality, two party data authentication, and data freshness, with low overhead and authenticated streaming broadcast respectively. While implementation and evaluation the authors assume that in the network individual sensors are untrusted, basic wireless communication is not secure, before deployment each node is given a master key which is shared with the base station. Experimentation has been performed on SmartDust nodes.

In [13], the authors presented the security enhancement SRTLD that uses the encryption and decryption with authentication of the packet header to supplement secure packet transfer. SRTLD [13] is the enhancement of RTLD by including security management module. SRTLD enhance the production of real random number by using a unique random generator function encrypted with mathematical function [13]. The output of the random function is used to encrypt specific header fields in the packet such as source, destination addresses, and packet ID. The data authenticity in SRTLD was done using an authentication procedure applied before decryption. In SRTLD, its assumed that each sensor node is static, aware of location, and sink is a trusted computing base [13]. SRTLD defends WSN from selective forwarding, sinkhole, Sybil, wormholes, and HELLO flood attacks. The MAC and physical layers in WSN are based on IEEE 802.15.4 which is designed for low rate communication.

Literature review concludes that the data security and routing designs in WSN do not work easily, due to the numerous constrains in WSN such as memory storage, power limitation and unreliable wireless communication. The aforementioned limitations should be considered when security based on routing is designed. The security measures

as we have discussed above have still lot of vulnerability and could not tackle the most common WSN routing attacks.

III. ARCHITECTURE OF PROPOSED MECHANISM

We enhance BIOSARP with random generator function encrypted with mathematical function [13]. The output of random generator function is used to encrypt specific header fields in the packet such as source, destination addresses and packet ID (Pkt_ID).

The encryption mechanism under E-BIOSARP generates and forwards a secure packet over WSN. If a malicious node takes the secure packet, it could not read the encrypted fields of secure packet. The encryption is performed with the help of dynamic mathematical computation. The random key encryption and decryption mechanism is developed based on the following assumptions:

- Pseudo random function as a function of master key and Pkt_ID, is stored in sensor node during program uploading.
- Hard mathematical function with its reverse computation is stacked in each sensor node before sensor deployment.
- Two master keys (k, k1) are inserted during program uploading into sensor nodes. Where k is used as a master key in all nodes for encryption and decryption purpose and k1 is used as a master key for a new node after WSN is established.

The encryption mechanism is explained with the help of state machine diagram as shown in Figure 3. A ciphertext packet is when received by routing management; the state immediately invokes decryption. Under decryption the algorithm decrypts Source Node ID (S_ID) and Destination Node ID (D_ID). Since, the authorized wireless node have our own encryption based random generator, thus it can develop the similar random key to decrypt packet based on the Pkt_ID and k.

The decryption function invokes authentication process for authentication. Onwards, the output of decryption process is checked by authentication process. The status is normal if the decryption process output is in between 0 and R. Finally, if status is normal the security module replay back to routing management to process the packet. Furthermore, if new wireless node needs to join WSN, the new R is encrypted by the same encryption mechanism with k1 as a master key in random function and transfer with control packet.

The autonomous security mechanism requires certain time at beginning to acquire knowledge. Until AIS maintains itself by building the network knowledge. As, in initialization phase WSN is unsecure and can be damaged, hacked or taken over by adversaries. As discussed in the previous sections that to secure WSN at the beginning stage, BIOSARP is additionally enriched with packet encryption and decryption inspired by human immune blood brain barrier (BBB) system [8, 9]. While communicating over WSN, E-BIOSARP encrypt and decrypt the header fields of data and control packets. Encryption and decryption algorithm is shown in Figure 4 and 5 respectively. The packet encryption and decryption starts by reading the S_ID and D_ID in the packet header. Whenever the packet is authenticated the node will further processes the packet or the packet is dropped.

In the encryption process S_ID, D_ID and Pkt_ID are extracted from the transmission packet header. Next, the pseudo random number is generated based on Pkt_ID and k. The encryption mathematical function is exploited before secure packet is sent. It is vital to note that the maximum size of encrypted filed is 4 bytes (231-1) and the encryption function may generate numbers greater than the maximum size of encrypted filed. In order to counter this problem, the module function will be utilized only once at the output of the encryption function as illustrated in Figure 4.

In the decryption process similarly, first S_ID, D_ID and Pkt_ID are extracted from the received packet header as shown in Figure 5. The pseudo random number is generated based on Pkt_ID and k. The encrypted field (S_ID and D_ID) is verified whether the encrypted field uses the modulo function. If the encrypted field employs modulo function, it will add to (231-1) once only.

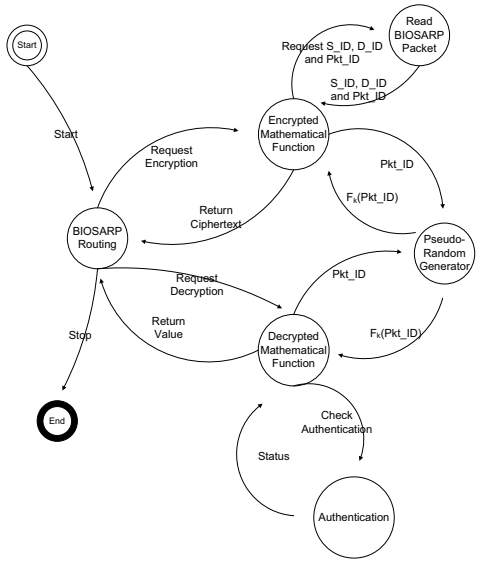


Figure 3. State Machine Diagram of Packet Encryption and Decryption

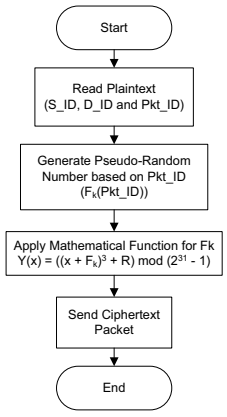


Figure 4. Flow Chart Diagram of Encryption with Authentication

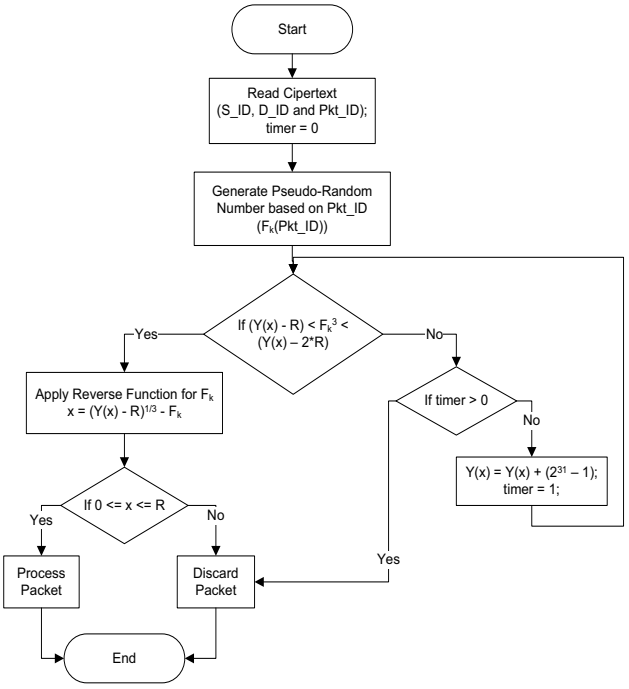


Figure 5. Flow Chart Diagram of Decryption with Authentication.

Then, the reverse of the encryption function is exercised followed by the authentication. If the output from the reverse process is between 0 and the number of sensor nodes in WSN, the packet arrive from a legal node and the received packet will be admitted. Otherwise, the received packet is discarded. The pseudo code of Encryption and Decryption algorithm is shown in Figure 6.

```
{
Switch (Encryption or Decryption)
{
Case 0:   // EncryptionRead packet header;
                        Encrypt S_ID and/or D_ID;
                        Send secure packet;
Break;
Case 1:   // Decryption          Read secure packet;
                        Extract S_ID and D_ID with Pkt_ID;
                        Decrypt S_ID and D_ID;
                        Implement authentication;
Break; }}
```

Figure 6. Pseudo Code

IV. Simulation Results

The proposed security mechanism is designed based on the assumptions that each wireless sensor node is static and the sink is a trusted computing base. The network parameters used to configure the WSN is given in Table 1. The network model used in this research conforms to IEEE 802.15.4 MAC and physical layers. Many-to-one traffic pattern is used which is common in WSN applications. This traffic is typical between multiple source nodes and a base station. In all simulations, each node updates its neighbor table every 180s. Network topology is configured similar to [13], as shown in Figure 7. Packet delivery ratio and normalized energy consumption are the metrics used to analyze the performance of E-BIOSARP.

TABLE I. Network Parameters To Simulate Security Mechanism

Propagation Model	Shadowing
path loss exponent	2.45
shadowing deviation (dB)	4.0
reference distance (m)	1.0
Low Rate WPAN	IEEE 802.15.4
phyType	Phy/WirelessPhy/802_15_4
macType	Mac/802_15_4
Operation mode	Non Beacon (unslotted)
Ack	Yes
CSThresh_	1.10765e-11 Hz
RXThresh_	1.10765e-11 Hz
freq_	2.4e+9 Hz
Initial Energy	3.3 Joule
Power transmission	1 mW
Transport layer	UDP
Traffic	CBR with Packet Size 70 bytes
Simulation Duration	300 seconds
Nodes	121
Region	80m x 80m
Source Nodes	120, 110, 100 and 90
Adversary Nodes	24, 25, 31 and 36

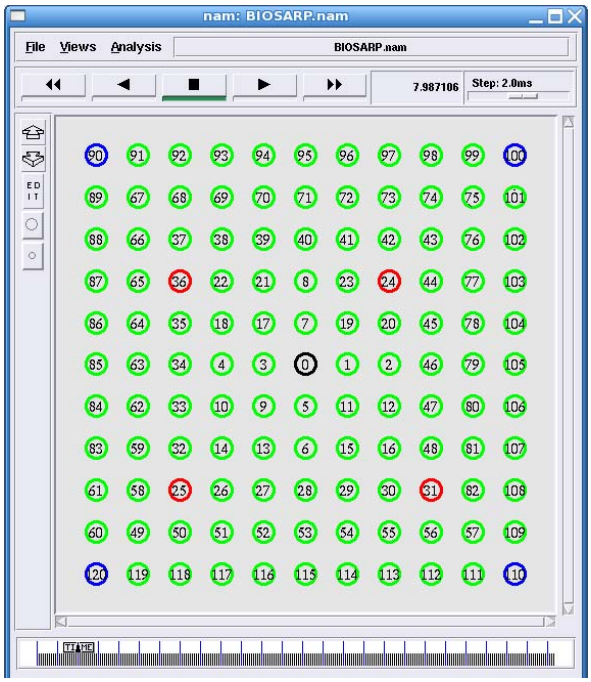


Figure 7. Network Simulation Grid (Sink Node (Black), Source Node (Blue), Malicious Node (Red) and Sensor node (Green))

A. Abnormalities and Attacks Countermeasures

Figure 8 shows the countermeasure against malicious packet with the help of E-BIOSARP that based on BBB technique. The mark in Figure 8 shows an unsecure packet received from the node 31 and it is dropped. The encryption and decryption mechanism helps even at the beginning stage of network. The countermeasures against the attacks generated by malicious nodes are explained in detail as follows.

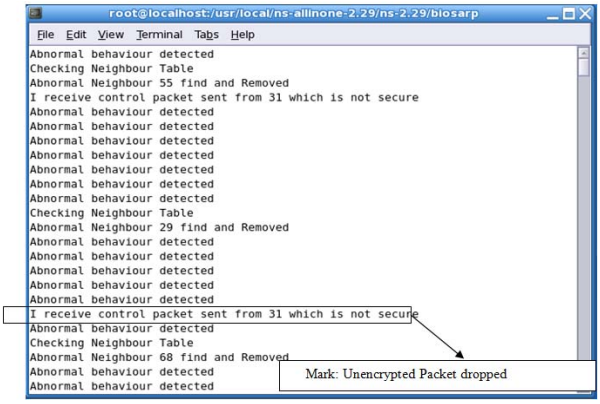


Figure 8. NS-2 Showing the Abnormality and Actions Taken Against Adversaries

- Spoofed, Altered or Replayed Routing Information Attacks

The malicious or adversary node targets the routing information between nodes as shown in Figure 9.

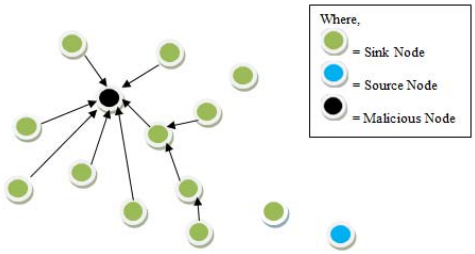


Figure 9. An Adversary Spoofing a Routing Update

E-BIOSARP prevents the sensor nodes from these attacks through the packet header encryption system based on BBB mechanism. When the sensor node transmit the packet it encrypts the header and while receiving also the E-BIOSARP checks that certain fields are encrypted with the right key or not. If not then the packet is directly dropped without opening as shown in Figure 8.

- Selective Forwarding and Acknowledgement Spoofing

Malicious node drops packets instead of forwarding and the neighboring node concludes that the current route has problem as the attacks as shown in Figure 10. In acknowledgment spoofing through feedback the malicious node convince the sender that weak link is now strong. E-BIOSARP save the network from these attacks with the help of header encryption system as shown in Figure 8.

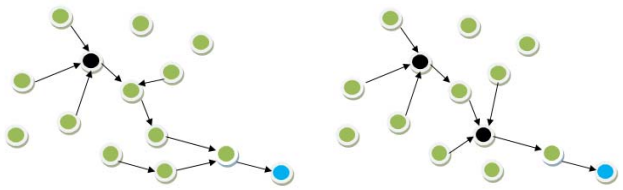


Figure 10. Selective Forwarding Attack by a) Single Malicious Node, b) Two Malicious Nodes

- Sybil Attack

In Sybil attack malicious node comes up with multiple IDs as shown in Figure 11. When these kinds of Request-To-Route (RTR) packets are received by E-BIOSARP, they are dropped due to different packet header as exposed in Figure 8.

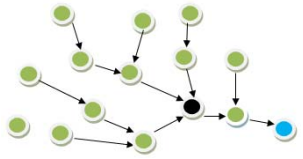


Figure 11. A Malicious Node with Multiple Identities Arise Sybil Attack

- Hello Flood Attack

In hello flood attacks as shown in Figure 12 also a laptop-class invader, which is broadcast with better signal strength, could convince nodes in WSN that the adversary is its neighbor. With the help of BBB the unencrypted packets will be dropped as shown in Figure 8. Hence, the chance forwarding data to non-self or hello flood generated node is negligible.

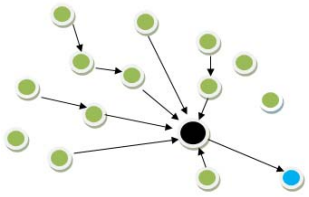


Figure 12. Hello Flood Attack

B. Influence of Increased Malicious Nodes and attacks on WSN

The routing protocol performance is affected when malicious nodes generates all kind of network layer attacks. The effect by increasing malicious nodes over WSN is elaborated under this section. In simulation study, 49 nodes are distributed in 80m2 region is conducted as in [13]. The 9.6 packets/s is fixed as the packet rate, whereas, the malicious nodes are increased from 4 to 20 wireless nodes. The network grid is shown in Figure 13, as the worst case scenario with 20 malicious nodes.

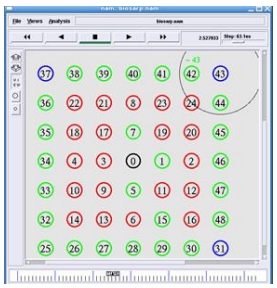
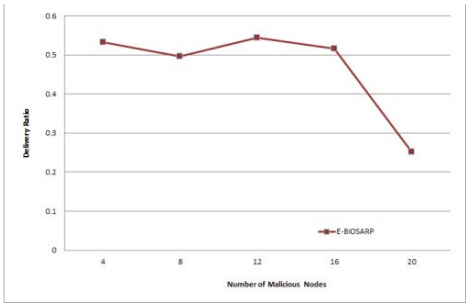


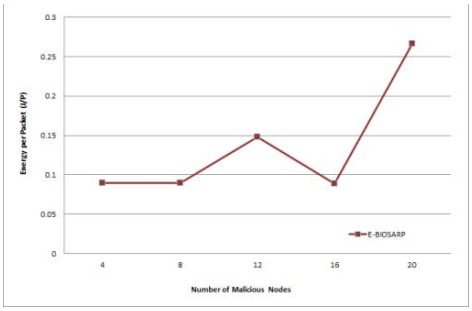
Figure 13. Increasing Compromised Nodes in Network Grid (Sink Node (Black), Source Node (Blue), Malicious Node (Red) and Sensor Node (Green))

The E-BIOSARP performance in terms of delivery ratio is reasonably constant as the number of malicious nodes is

increased. E-BIOSARP deals with malicious node as vulnerability. Via Figure 14(a) we see that the delivery ratio starts declining as, when the malicious nodes crosses 16, due to communication problem occurs from source nodes 43, 31 and 37 to sink as given in Figure 13. The battery power consumption grows as shown in Figure 14(b), because hop to hop distance becomes bigger and to communicate on large distances the transmitter works with maximum power.



(a) Delivery Ratio



(b) Power Consumption

Figure 14. Influence of Malicious Nodes in Network Performance

C. Processing Time Comparison

The security processing time per hop in routing protocol is very important parameter as it affects the performance in terms of energy consumption and delivery ratio. SRTLD requires less processing time as compared to TinyHash, TinySec-AE, TinySec-Auth, EBSS, TEA LBRS-Auth [13]. Figure 15 shows E-BIOSARP utilizes less processing time as compared to SRTLD and SPINS. This is primarily due to the simplicity of the autonomous routing algorithm. Hence, E-BIOSARP is effective in applications where data is having short time to live (TTL).

D. Delivery Ratio Comparison

The output is graphically represented via Figure 16 that shows the delivery ratio by E-BIOSARP is higher as compared to the SRTLD routing protocols. Delivery ratio is increased because the processing time required to entertain the packets is very less as compared to SRTLD as shown in Figure 15. The advantage of less processing time ultimately helps in decreasing the delay while transferring data packets from source to destination securely. Furthermore, the result demonstrates that when malicious traffic is involved in wireless sensor network the throughput decreases.

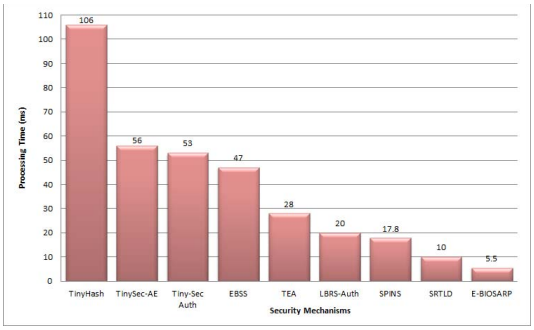


Figure 15. Processing Time Comparison

The proposed mechanism minimizes the broadcast and in overall the processing time that helps in reducing battery power consumption and processing delays. The utilization of resources is decreased by avoiding rediscoveries, replies, and recalculations.

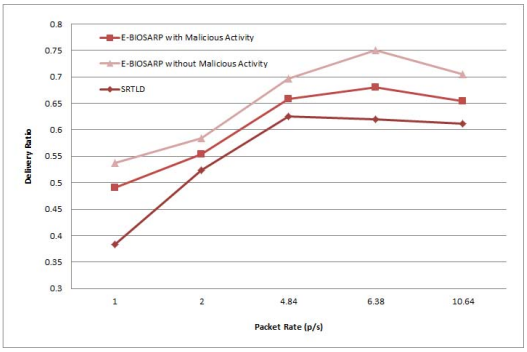


Figure 16. Delivery Ratio Comparison

E. Energy Consumption Comparison between E-BIOSARP and SRTLD

The energy required to process every packet in case of SRTLD is higher as compared to E-BIOSARP as shown in Figure 17. Energy consumption is reduced in the case of E-BIOSARP that is first of all due to less data encryption processing time and secondly because of reduced rediscovery process. Figure 17 additionally show that weather WSN has malicious nodes or not, the energy consumption rate of E-BIOSARP is almost same, which shows the efficiency of the proposed mechanism.

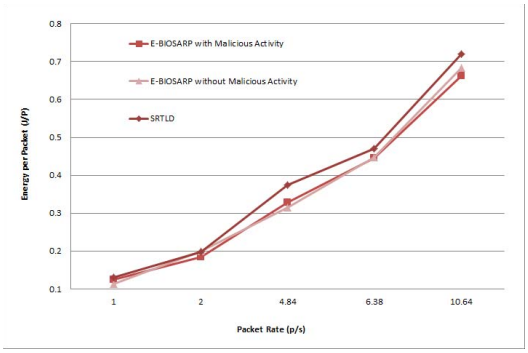


Figure 17. Energy Consumption Comparison

V. Conclusion And Future Work

The recent autonomous secure routing protocol (BIOSARP) for WSN requires certain time to maintain and secure the network communication. If the required monitoring area already contains malicious nodes and activity, then WSN at the time of deployment is totally open for adversaries and can be taken over easily. To secure WSN in the beginning until initialization completes, the BIOSARP is enhanced with random key encryption and decryption mechanism.

The encryption process reads packet ID (Pkt_ID), source ID (S_ID) and destination ID (D_ID) from the packet header. The pseudo random number is generated based on Pkt_ID and master key in all nodes (k) and encrypt the fields S_ID and D_ID in packet header. While receiving side the packet header fields S_ID and D_ID is decrypted on the base of Pkt_ID and k. Packet is further processed if authenticated else discard. Thus, E-BIOSARP can provide countermeasures against spoofed, altered or replayed routing information attacks, selective forwarding, acknowledgement spoofing, sybil attack and hello flood attack.

The influence of increasing compromised nodes in network performance has been presented. E-BIOSARP, in overall provides much better output in front of SRTLD and SPINS. Additionally, result presents the malicious activity and shows the energy consumption rate, which explains the efficiency of the proposed mechanism. Hence, the result successfully shows the accuracy, efficiency and stability of E-BIOSARP. Hence, E-BIOSARP is able to secure WSN from the beginning of wireless sensor network deployment.

Our future work involves the testing of random key based efficient encryption mechanism in the realtime WSN experimental testbed.

Acknowledgment

Sincerest gratitude to Ministry of Higher Education (MOHE), Malaysia and Center of Excellence in Information Assurance (CoEIA), King Saud University (KSU). Thank you to the officials and senior researchers at Center of Excellence in Information Assurance (CoEIA), King Saud University (KSU) for their invaluable help and guidance.

References

[1] A. Cerpa, J. L. Wong, L. Kuang, M. Potkonjak, and D.Estrin, "Statistical Model of Lossy Links in Wireless Sensor Networks," in *ACM/IEEE IPSN*, Los Angeles, USA, 2005.

[2] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *Wireless Communications, IEEE,* vol. 11, pp. 6- 28, 2004.

[3] K. Saleem, N. Fisal, M. S. Abdullah, and S. Hafizah, "Biological Inspired Secure Autonomous Routing Mechanism for Wireless Sensor Networks," *International Journal of Intelligent Information and Database Systems (IJIIDS),* 2010.

[4] J. P. Walters and Z. Liang, "Wireless Sensor Network Security: A Survey," in *Security in Distributed Grid and Pervasive Computing*, ed: Auerbach Publications, CRC Press, 2007, pp. 368-403.

[5] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks,* vol. 1, pp. 293-315, 2003.

[6] A. K. Pathan, H. W. Lee, and C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges," in *Proceedings of 8th IEEE ICACT 2006*, Phoenix Park, Korea, 2006, pp. 1043-1048.

[7] K. Saleem, N. Fisal, M. A. Baharudin, A. A. Ahmed, S. Hafizah, and S. Kamilah, "Ant Colony Inspired Self-Optimized Routing Protocol based on Cross Layer Architecture for Wireless Sensor Networks," *WSEAS TRANSACTIONS on COMMUNICATIONS (WTOC),* vol. 9, pp. 669-678, 2010.

[8] T. O. Kleine and L. Benes, "Immune surveillance of the human central nervous system (CNS): Different migration pathways of immune cells through the blood–brain barrier and blood–cerebrospinal fluid barrier in healthy persons," *Cytometry Part A,* vol. 69A, pp. 147-151, 2006.

[9] G. J. Swanson, "The Central Nervous System of Vertebrates," *Trends in Neurosciences,* vol. 21, pp. 538-539, 1998.

[10] C. H. Lim, "LEAP++: A Robust Key Establishment Scheme forWireless Sensor Networks," in *The 28th International Conference on Distributed Computing Systems Workshops*, Beijing, China, 2008.

[11] H. Wang, B. Sheng, C. C. Tan, and Q. Li, "Comparing Symmetric-key and Public-key based Security Schemes in Sensor Networks: A Case Study of User Access Control," in *The 28th International Conference on Distributed Computing Systems*, Beijing, China, 2008.

[12] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks,* vol. 8, pp. 521-534, 2002.

[13] A. A. Ahmed and N. F. Fisal, "Secure real-time routing protocol with load distribution in wireless sensor networks," *Security and Communication Networks,* vol. 4, pp. 839-869, 2011.