International Journal of Electrical and Electronics Engineers

Vol. No. 9, Issue No. 01, January-June 2017

ISSN (O) 2321-2055
ISSN (P) 2321-2045

Security in WSN using Polynomial And SAMA Techniques

Deepika[1], Ms. Kusum Dalal[2]

[1]M.Tech. Scholar, [2]Assistant Professor,

Department of Electronics and Communication Engineering, DCRUST, Murthal (India)

ABSTRACT

In wireless sensor networks (WSNs), security has become a topic of vital importance these days. Message authentication is one of the most effective ways to prevent unauthorized and corrupted traffic from being forwarded in WSNs. To provide this service, various authentication schemes have been proposed earlier for protecting communication authenticity and integrity in WSNs. After analyzing some of the message authentication protocols for WSNs it was found that most of them suffer threshold limitation problem or could only provide end-to-end authentication. In this paper, these problems are being addressed through ECC technology. This scheme not only provides hop-by-hop authentication, but also allows any node in WSNs to transmit an unlimited number of messages without suffering the threshold problem. In addition, this scheme can also provide message source privacy. This scheme has also been compared with the bi-variate polynomial scheme through simulations using MATLAB.

Keywords- Elliptic curve cryptography (ECC), Source anonymous message authentication (SAMA) scheme, source privacy, symmetric-key cryptosystem, public-key cryptosystem, Wireless sensor networks (WSNs),

I. INTRODUCTION

Wireless sensor network (WSN) comprises of a large number of static or mobile sensor nodes which form the wireless network using self-organization and multi-hop method. Its basic purpose is to collaborate detection, processing and transmitting the object monitoring information in those areas where the network converges [1]. The sensor node, sink node and the user node are the three elements of sensor networks. Sensor node is the foundation of the whole network which is responsible for the perception of data, data processing, storage of data and its transmission. The sensor node can sense many environmental conditions, including temperature and humidity, pressure, light condition, vehicle movement, mechanical pressure strength, the speed of the airflow direction and other characteristics. The main features of WSNs are self-organization, multi-hop route, dynamic network topology, data-centric and security problem. The nodes of the WSN have the automatic networking function and the nodes can communicate with each other. In the application of wireless sensor network, typically the sensor nodes are placed somewhere with no base network facility, such as a vast area of virgin forest, or the danger area where people cannot reach. When a node cannot directly communicate with the gateway, it requires other nodes to transmit data, so the network data transmission is a multi-hop routing. There are a large number of sensor nodes in WSN and often need to be arranged in a specific monitoring area. The hardware resources of sensor node are limited because of the size and cost constraints. So its computing power, storage capacity is relatively weak. Mobile communication network or Ad-hoc network mainly considers how to improve the network transmission capacity under current conditions, which is to provide users with a sufficient bandwidth, safe and reliable transmission channel. As wireless sensor networks uses wireless transmission, so the monitoring data is easy to be intercepted, or even confuse users after tampering. After a large number of sensor nodes are captured, the enemy may use them to destroy the existing network. Therefore, in the design of WSNs, security problem is the main focus of the study.

WSNs are designed to operate unattended for long periods of time, so recharging or replacement of battery seems to be infeasible or impossible. Hence, computationally intensive cryptographic algorithms such as public-key cryptosystems and large scale broadcasting-based protocols may not be quite suitable for WSNs. In the wireless sensor domain, anybody with an appropriate wireless receiver can monitor and intercept the sensor communication [2]. In addition, the adversaries may use expensive radio transceivers and powerful workstations to interact with WSNs to get traffic information from a distance because they are not restricted to use sensor network hardware. In the worst case, adversaries may be able to take control of some sensor nodes, compromise the cryptographic keys and reprogram some sensor nodes. This makes privacy preserving communication in WSNs a very challenging research task. Unfortunately, to optimize the sensor nodes for the limited capabilities and application specific nature of WSNs, traditionally, security requirements were largely ignored. This leaves WSNs vulnerable to security attacks [3].

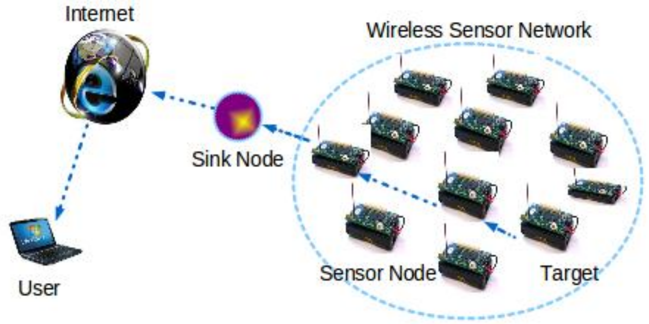

Fig.1: Wireless Sensor Network

Source-location privacy is an important security issue for WSNs. Lack of location privacy can cause exposure of significant information about traffic carried on the network and the physical world entities. While confidentiality of a message can be ensured through content encryption, it is much more difficult to adequately address pattern and source-location information. Using certain equipments to monitor the transmission direction of any detected message, adversaries can easily trace back to the source node hop by hop or deduce the location of the source node through traffic analysis [4]. Besides source-location privacy, non-repudiation is another property that cannot be ignored for source privacy in wireless communication. Without the non-repudiation, not only attackers, but also network administrators cannot get any information about the source. This makes managing operations almost impossible for network administrators. Lack of non-repudiation also prevents administrators from distinguishing valid messages from fake and unauthorized messages set by attackers. Therefore, attackers could carry out flooding attack to disable the wireless communications in WSNs. To summarize, there are two aspects that need to be considered for source privacy: source-location privacy and anonymous source authentication. To make secure data transmission over networks cryptography is used. Cryptography is a method used to encrypt, or scramble, the contents of a file in such a way that only those with the knowledge of how to decrypt, or unscramble, the contents can read them. The algorithm being selected for cryptography must fulfill the conditions of integrity protection, conventional message authentication and digital signatures.

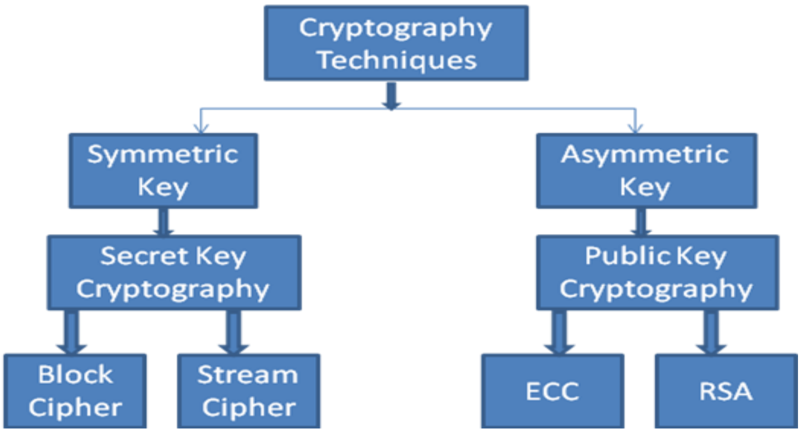

Fig.2: Types of Cryptography Techniques

The paper is organized as follows: Routing protocols for WSNs are discussed in section II. In section III, various attacks in WSNs are being explained. Source Anonymous Message Authentication (SAMA) scheme on elliptic curve is discussed in section IV. Section V explains the simulation results. Conclusion is given in section VI.

II. ROUTING PROTOCOLS FOR WSNs

Important applications of sensor networks are data gathering and processing. All the data collected by the individual sensor nodes need to be sent to the sink node, from where it is accessible by the end user. The distributed nature and dynamic topology of WSNs introduces some special requirements of routing protocols that should be met. Hence, various routing techniques are introduced for WSNs based on certain characteristics like, in-network processing, data aggregation and processing, position of node, clustering nodes, energy consumption, etc. The routing protocols for WSNs can be categorized into data-centric or flat-based, hierarchical or cluster-based and location-based, depending on the network structure. They can also be divided into multipath based, QoS-based depending on how the protocol operates. By having a review of various routing protocols, a comparison can be made between various routing protocols which show that the hierarchical protocols are proved to be the energy efficient routing protocols. So, data communication is sustained by using LEACH protocol in the network [17].

A. Hierarchical Protocols

Hierarchical clustering is an energy efficient communication protocol that can be used by the sensors to report their sensed data to the sink. Some of the layered protocols in which a network is composed of several clumps (or clusters) of sensors are described below.

1) LEACH: Low-Energy Adaptive Clustering Hierarchy, i.e. LEACH is the hierarchical clustering algorithm for WSNs which was proposed for reducing power consumption. Here, various clusters of the sensor nodes are being formed on basis of the received signal strength and use the local cluster heads as routers to the sink. This leads to saving of energy since the transmissions will only be done by cluster heads rather than all sensor nodes.

Optimal number of cluster heads is estimated to be approximately 5% of the total number of nodes. All the data processing functions such as data fusion and aggregation are local to the cluster. The cluster heads change randomly over time in order to balance the energy dissipation of the nodes. This decision that which node will become a cluster head is made by the node choosing a random number between 0 and 1. The node becomes the cluster head for the current round if number is less than the threshold. The nodes start to die randomly and the dynamic clustering thus further increases the lifetime of the system. LEACH is distributed completely and requires no global knowledge of the network. However, LEACH uses single-hop routing in which each node can transmit directly to the sink and the cluster-head. Thus limiting its use for large regions. Also, the idea of dynamic clustering brings extra burden, like, head changes, advertisements etc., which may nullify the gain in energy consumption [19].

*2) **PEGASIS:*** Power-Efficient Gathering in Sensor Information Systems, i.e. PEGASIS is an extension of the LEACH protocol. In PEGASIS, various sensor nodes form chains so that each node can transmit and receive from a neighboring node and only one node is selected from that chain to transmit data to the base station (sink). The data is aggregated while it moves from node to node, and eventually sent to the base station. The chain construction is performed in a greedy way. Unlike LEACH, there is no cluster formation in PEGASIS but it uses only one node in a chain to transmit to the base station instead of using multiple nodes. The sensor also transmits to its local neighbors in the data fusion phase instead of sending directly to its cluster head, as in the case of LEACH. Here, the construction phase considers that the sensors already have global knowledge about the network especially, the positions of the sensors, and use a greedy approach. The same approach is being used when a sensor fails due to low battery power; the chain is constructed by bypassing the failed sensor. In each round, a randomly chosen sensor node transmits aggregated data to the sink, thus reducing the per round energy consumption as compared to LEACH [20].

III. ATTACKS IN WSNs

WSN consists of a large number of small and low cost sensor nodes which are randomly deployed in an area. The sensor nodes have computational capability to carry out simple computations and transmit the required information [21]. These nodes transmit information to the sink node that aggregates the entire information received from other nodes and generates a summary data to be transmitted to another network. These sensor nodes can collectively monitor physical and environmental conditions like pressure, temperature, humidity and sound vibrations. Such features ensure a wide range of applications for wireless sensor network such as military, medical, industrial, disaster relief operations, environmental monitoring, traffic surveillance, agriculture, infrastructure monitoring [21][22]. Since the majority of sensor nodes are deployed in hostile environment, they are susceptible to various attacks that are caused by malicious or compromised nodes in the network. The malicious nodes can alter the normal behavior of the network, tamper with the node's hardware and software, transmit false information, or drop the required information. Hence, security of WSN becomes a critical issue.

A. Types of attacks

The attacks on wireless sensor networks can be categorized into several forms but there are basically two main types of attacks that an intruder may adopt.

*1) **Passive Attack:*** A passive attack involves monitoring and listening of the data stream but doesn't involve modification of the data stream. Passive attacks do not cause direct harm to the network as they cannot modify the data. Attack against privacy is a passive attack [22]. The goals and effects of this kind of attacker include –

- Eavesdropping, gathering and stealing information;
- Compromised privacy and confidentiality requirements;
- Storing energy by selfish node and to avoid from cooperation;
- The WSN functionality degradation;
- Network partition by non-cooperate in operations [23].

*2) **Active Attack:*** An active attack involves monitoring, listening and modification of the data stream by the malicious nodes/adversaries prevailing inside or outside the network. Active attacks cause direct harm to the network because they can manipulate the data stream [22]. Some of the goals and effects of these attacks are:

- The WSN functionality disruption;
- The WSN performance degradation;
- Sensor nodes destruction;
- Data alteration;
- Inability in use the WSN's services;
- Obstructing the operations or to cut off certain nodes from their neighbours.

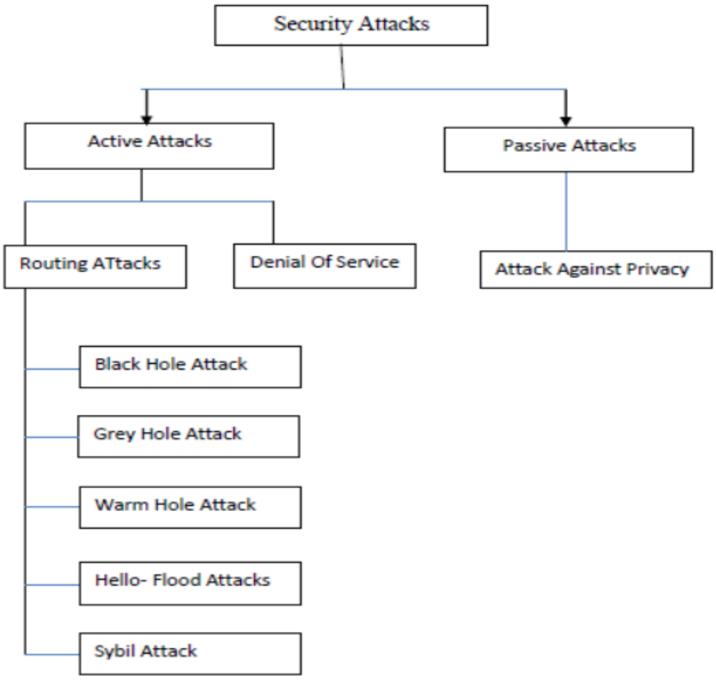

Fig. 3: Types of attacks

IV. SOURCE ANONYMOUS MESSAGE AUTHENTICATION (SAMA) SCHEME ON ELLIPTIC CURVE

The main idea is that for each message m to be released, the message sender, or the sending node, generates a source anonymous message authentication for the message m. The generation is based on the MES scheme on elliptic curve. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS individually. In this scheme, the entire SAMA generation requires only three steps, which link all non-senders and the message sender to the SAMA alike. In addition, the design enables the SAMA to be verified through a single equation without individually verifying the signatures.

A. MES Scheme on Elliptic Curve

Let p > 3 be an odd prime. An elliptic curve E is defined by an equation of the form:

$$\boxed{E : y^2 = x^3 + ax + b \bmod p}$$

where a, b ∈ F_p, and 4 a^3 + 27 b^2 /≡ 0 mod p. The set E(F_p) consist of all points (x, y) ∈ F_p on the curve, together with a special point O called the point at infinity.

Let G = (x_G ,y_G) be a base point on E(F_p) whose order is a very large value N. User A selects a random integer $d_A \in [1, N-1]$ as his private key. At that point, he can process his public key Q_A from $Q_A = d_A \times G$.

1) *Signature Generation Algorithm:* For Alice to sign a message m, she follows these steps –

- Select a random integer k_A, $1 \leq k_A \leq N - 1$.
- Calculate r = x_A mod N, where (x_A, A) = k_AG. If r = 0, backtrack to step 1.
- Calculate $h_A \overset{l}{\leftarrow}$ h(m, r), where h is a cryptographic hash function, such as SHA-1, and $\overset{l}{\leftarrow}$ means the l leftmost bit of the hash.
- Calculate s = rd_A h_A +k_A mod N. If s = 0, go back to step 2.
- The signature is the pair (r, s). When computing s, the string ha resulting from h(m, r) shall be converted into an integer.

2) *Signature Verification Algorithm:* For Bob to authenticate Alice's signature, he must have a copy of her public key Q_A –

- Check that Q_A/ = O, otherwise invalid
- Check that Q_A lies on the curve
- Check that nQ_A = O

After that, Bob follows these steps to verify the signature –

- Verify that r and s are integers in [1, N — I]. If not, the signature is invalid.
- Calculate $h_A \overset{l}{\leftarrow}$ h(m, r), where h is the same function used in the signature generation.
- Calculate ($x_{1,2}$) = sG − rh_A Q_A mod N.
- The signature is valid if r = $x_1$mod N, invalid otherwise.

In fact, if the signature is correctly generated, then

($x_{1,2}$) = sG - rh_A Q_A

= (rd_A h_A + k_A)G - rh_A Q_A

= k_A G + $rh_A$$Q_A$ - rh_A Q_A

= k_A G.

Therefore, we have x_1= r and the verifier should accept the signature.

B. SAMA scheme on Elliptic Curve

Assume that the message sender (say Alice) wishes to transmit a message m secretly from her network node to any other nodes. The AS includes n members, $A_{1,2}$……A_n, e.g., S = {A_1,A_2,….A_n}, where the actual message sender Alice is A_t, for some value t, $1 \le t \le n$. In this dissertation, we will not distinguish between the node A_i and its public key Qi. Consequently, we also have $S = \{Q_{1,2},\ldots Q_n\}$.

1) Authentication generation algorithm: Suppose m is a message to be transmitted.

The private key of the message sender Alice is d_t, $1 < t < N$. To generate an efficient SAMA for message m, Alice performs the following three steps:

- Select a random and pairwise distinctive k_i for each $1 \le i \le n - 1$, $i \ne t$, and compute r_i from $(r_{i,i}) = k_i$ G.
- Choose a random $k_i \in Z_p$ and compute r_t from

$(r_t\ y_t) = k_t G - r_i \sum_{i \neq t} r_i\ h_i\ Q_i$ such that $r_t \ne 0$ and $r_t \ne r_i$ for any $i \ne t$; where $h_i \overset{l}{\leftarrow}$ h(m,r_i).

- Compute $s = k_t + \sum_{i \neq t} k_i + r_t\ d_t\ h_t \bmod N$.

The SAMA of the message m is characterized as:

$S(m) = (m, S, r_1, y_1,\ldots,r_n, y_n, s)$.

2) Verification Algorithm: Verification algorithm for Bob to verify an alleged SAMA (m, S, r_1, y_1,…,r_n, y_n, s), he must have a copy of the public keysQ_1,…,Q_n. Then he checks:

- Check that $Q_i \ne O$; i = 1, ... ,n, otherwise invalid
- Check that Q_i, i = 1, ... , n lies on the curve
- Checks that $nQ_i = O$, i = 1, ... , n

After that, Bob follows these steps:

- Verify that r_i ,$_i$, i = 1, ... , n, and s are integers in [1,N − 1]. If not, the signature is invalid.
- Calculate $h_i \overset{l}{\leftarrow}$ h(m, r_i), where h is the same function used in the signature generation.
- Calculate $(x_0, y_0) = sG - \sum_{i=1}^{n} r_i\ h_i\ Q_i$
- The signature is valid if the first coordinate of $\sum_i (r_i\ y_i)$ equals x_0, invalid otherwise.

In fact, if the SAMA has been correctly generated without being modified, then we compute

$(x_0, {}_0) = sG - \sum_{i=1}^{n} r_i\ h_i\ Q_i$

$= (k_t + \sum_{i \neq t} k_i + r_t\ d_t\ h_t)G - \sum_i r_i\ h_i\ Q_i$

$= \sum_{i \neq t} k_i\ G + (k_t\ G - \sum_{i \neq t} r_i\ h_i\ Q_i)$

$= \sum_{i \neq t} (r_i\ y_i) + (r_t\ y_t)$

$= \sum_i (r_i\ y_i)$

Therefore, the verifier should always accept the SAMA

V. RESULTS AND DISCUSSIONS

A. Tool Used

The tool being used for the simulation is MATLAB (R2014a), developed by Math Works. It is an interactive software package which is mainly used for numerical computing.

B. Parameters Used

1) Energy Consumption: It is measure of energy consumed at nodes of the network. This shows the energy consumed by the nodes in total rounds.

2) Throughput: Throughput is the rate of production or the rate at which something can be processed. Throughput is the measure of comparative effectiveness of a process or an operation.

*3) Delivery ratio:*Ratio of number of packets delivered against the number of packets sent.

4) Memory Consumption: It is the amount of memory consumed by the nodes to store and processing the network information.

***C.* Simulation Results of Polynomial Technique**

1) Network and Possibility of Intruders Attack: Here, link between intruder node and other nodes is shown by black color and connection between sink node and other nodes is shown by red color. Maximum network range is 15m and maximum distance between two nodes is 10m. The distance of the nodes from intruder node is less than 10 m, is shown by yellow color. So the nodes close to the intruder node have more probability of being hacked by the intruder node than other nodes. The energy of all the nodes is E=0.5 and the probability of the node being dead is P=0.2.

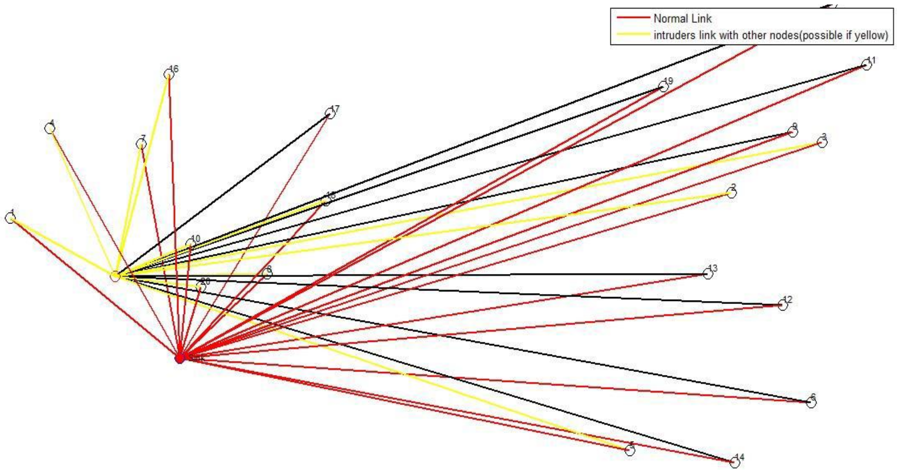

Fig.4: Network and possibility of intruders attack

2) Relation between intruder node, sink node and other nodes: The red color is for the intruder node and link between the sink node and nodes is shown with black color. Here, node no.9 is hacked and its identity is stolen by the intruder node, known as Sybil attack.

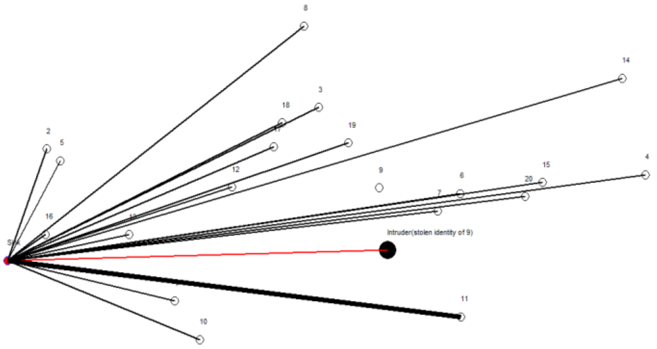

Fig.5: Relation between intruder, sink node and other nodes

3) Dead Nodes vs. Rounds: Here, we have taken 2000 round and after approx. 400 rounds the energy of nodes starts decreasing and upto approx. 1580 rounds all nodes are dead. So after this, communication will be stopped.

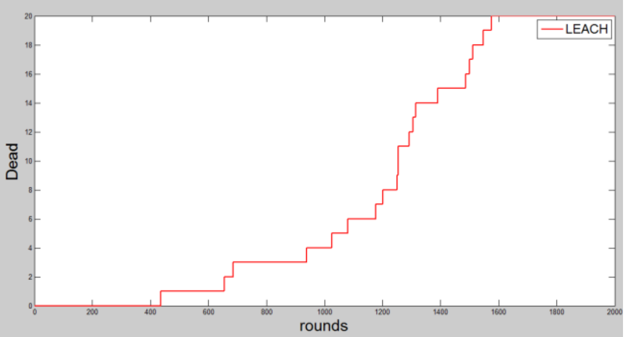

Fig.6: Dead nodes vs. rounds

4) Percentage of alive nodes vs. rounds: After approx. 1580 rounds all nodes are dead thus network is left with 0% alive nodes.

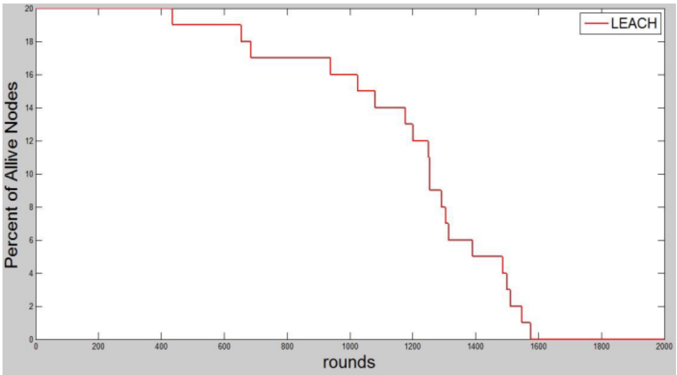

Fig.7: Percentage of alive nodes vs. rounds

5) Energy vs. rounds: After approx. 1580 rounds all the energy is consumed by the nodes thus leaving the whole network dead.

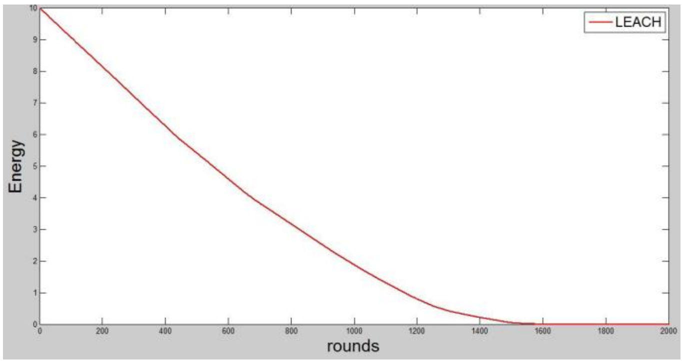

Fig.8: Energy vs. Rounds

6) Throughput vs. Rounds: This graph shows that the data is processed or communicated efficiently upto how much rounds.

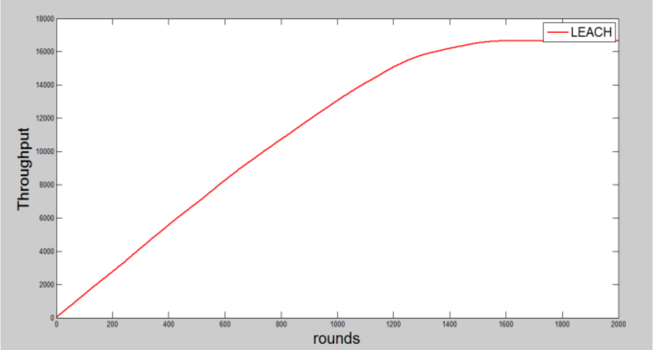

Fig.9: Throughput vs. rounds

D. Simulation results of SAMA technique

1) Dead vs. Rounds: We have taken 2000 rounds and after approx. 440 rounds, the energy of nodes starts decreasing and upto approx. 1600 rounds all nodes are dead. So after this, communication will be stopped as all nodes are dead in the network. So, network using SAMA technique conserves more energy than using polynomial technique.

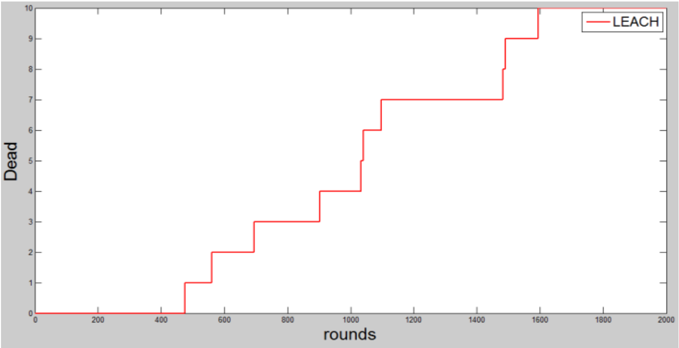

Fig.10: Dead vs. Rounds

2) Percentage of alive nodes vs. rounds: After approx. 1600 rounds all nodes are dead thus network is left with 0% alive nodes.

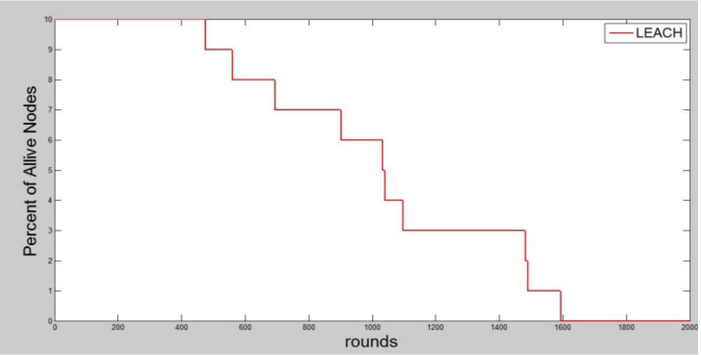

Fig.11: Percentage of alive nodes vs. Rounds

3) Energy vs. rounds: After approx. 1600 rounds all the energy is consumed by the nodes while communicating and thus leaving the whole network dead.

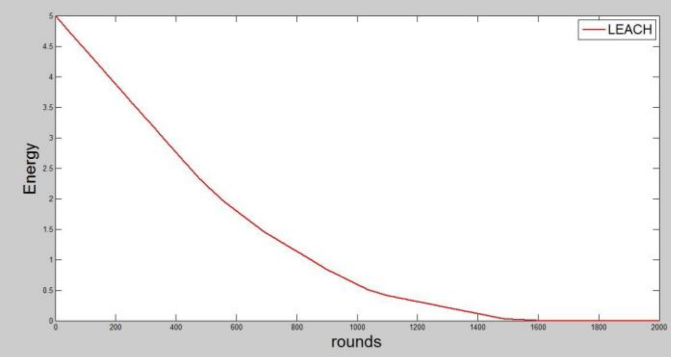

Fig.12: Energy vs. Rounds

4) Throughput vs. Rounds: Throughput is the measure of comparative effectiveness of a process or an operation.

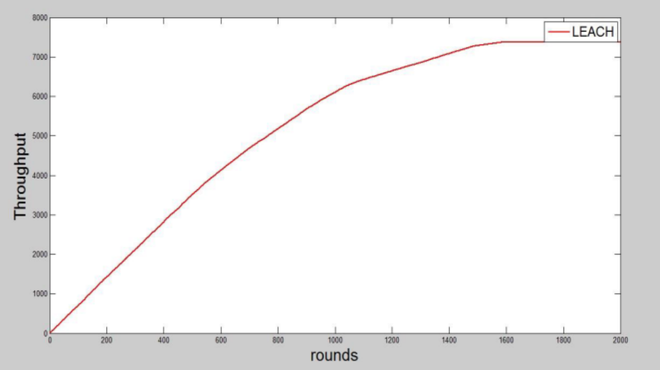

Fig.13: Throughput vs. Rounds

The simulation results demonstrate that our proposed scheme has a much lower energy consumption and the delivery ratio of our scheme is slightly better than the bivariate polynomial-based scheme. Morever, the overall memory consumption for the bivariate polynomial-based scheme is at least 5 times larger than our proposed scheme.

VI. CONCLUSION

In this paper, source anonymous message authentication scheme (SAMA) based on elliptic curve cryptography (ECC) is implemented using MATLAB software for the purpose of security of WSN. While ensuring message privacy, SAMA can be applied to any messages to provide hop-by-hop message content authenticity without the weakness of the built-in threshold of the polynomial-based scheme. Both theoretical and simulation results, conducted using MATLAB, show that, in comparable scenarios this proposed scheme is more efficient than the bivariate polynomial-based scheme in terms of energy consumption, and overall throughput. The results also demonstrate that the proposed scheme is secure with light overhead. In future, energy and security are both important design issues for WSNs. An interesting research topic that can be investigated is to develop a novel secure and energy aware routing protocol that can address these two issues concurrently through balanced energy consumption and probabilistic random walking. Based on the tradeoff relationship between security and energy, this protocol should provide tunable security level and energy consumption pattern. More detailed further researches in these supportive topics can be carried out.

REFERENCES

[1] Ming Liu, Jiannong Cao,et. al., “An Energy-aware Routing Protocol in Wireless Sensor Networks”, Sensors, vol. 9, pp. 445-462, 2009.

[2] Shiwei Zhang and Haitao Zhang, “A Review of Wireless Sensor Networks and its Applications”, “Automation and Logistics(ICAL), 2012 IEEE International Conference on ”, pp. 386, August 2012

[3] J.P. Walters, Z. Liang, W. Shi, V. Chaudhary, “Wireless Sensor Network Security: A Survey”, “Security in Distributed”, Grid and Pervasive Computing, pp.3-5, 10-15, 2006.

[4] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks," in IEEE Symposium on Security and Privacy, 2004.

[5] S. William, Cryptography and Network Security: Principles and Practice , 2nd edition, Prentice-Hall, 1999.

[6] Ayushi,” A Symmetric Key Cryptographic Algorithm”,”International Journal of Computer Applications”, Vol 1 – No. 15, pp. 2, 2010

[7] B.Schneier. Applied Cryptography, John Wiley and Sons, second edition, 2012.

[8] V. Miller, “Uses of elliptic curves in cryptography”, “Advances in Cryptology -CRYPTO'85”, LNCS 218, pp.417-426, 2011.

[9] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, “Perfectly-secure key distribution for dynamic conferences,” in Advances in Cryptology - Crypto’92, Lecture Notes in Computer Science Volume 740, pp. 471–486, 1992.

[10] W. Zhang, N. Subramanian, and G. Wang, “Light-weight and compromise resilient message authentication in sensor networks,” in *IEEE INFOCOM*, (Phoenix, AZ.), April 15-17 2008.

[11] D. Pointcheval and J. Stern, “Security proofs for signature schemes,” in Advances in Cryptology – EUROCRYPT, Lecture Notes in Computer Science Volume 1070, pp. 387–398, 1996.

[12] K. Nyberg and R. A. Rueppel, “Message recovery for signature schemes based on the discrete logarithm problem,” in Advances in Cryptology - EUROCRYPT, Lecture Notes in Computer Science Volume 950, pp. 182– 193, 1995.

[13] H. Wang, S. Sheng, 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 IEEE ICDCS, (Beijing, China), pp. 11–18, 2008.

[14] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks," in IEEE Symposium on Security and Privacy, 2004.

[15] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in IEEE Symposium on Security and Privacy, May 2000.

[16] C. K. Wong and S. S. Lam, "Digital signatures for flows and multicasts," IEEE/ACM Trans. Netw., vol. 7, no. 4, pp. 502-513, 1999.

[17] Kemal Akkaya and Mohamed Younis, “A Survey on Routing Protocols for Wireless Sensor Networks”, Ad hoc Networks, vol. 3, no. 3, pp. 325-349, May 2015.

[18] Rajashree.V.Biradar, V.C. Patil, et. al., “Classification And Comparison Of Routing Protocols In Wireless Sensor Networks”,”UbiCC Journal”,Vol-4, pp. 708-709.

[19] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient Communication Protocol for Wireless Microsensor Networks”, in IEEE Computer Society Proceedings of the Thirty ThirdHawaii International Conference on System Sciences (HICSS '00), Washington, DC, USA, vol. 8, pp. 8020, Jan. 2011.

[20] S. Lindsey and C.S. Raghavendra, “PEGASIS: Power-efficient Gathering in Sensor Information System”, Proceedings IEEE Aerospace Conference, vol. 3, Big Sky, MT, pp. 1125-1130, Mar. 2012.

[21] Mohamed-Lamine Messai,” Classification of Attacks in Wireless Sensor Networks”,” International Congress on Telecommunication and Application’14 University of A.MIRA Bejaia, Algeria”, 23-24 APRIL 2014

[22] Deepali Virmani, et. al.,” Routing Attacks in Wireless Sensor Networks: A Survey”,” International Journal of Computer Science and Information Technologies (IJCSIT)”,Vol.5(2),pp.2666-26667,2014.

[23] Dr. Shahriar Mohammadi, et.al ,” A Comparison of Physical Attacks on Wireless Sensor Networks”,” International Journal of Peer to Peer Networks (IJP2P)”, vol. 2,No. 2,pp.29-30, April 2011.

[24] Wensheng Zhang and Nalin Subramanian,” Lightweight and Compromise-Resilient Message Authentication in Sensor Networks”,” IEEE INFOCOM”,2008.

[25] A. S.Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in PERCOM '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, (Washington, DC, USA), pp. 324-328, IEEE Computer Society, 2005

[26] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, "State of the art in ultra-low power public key cryptography for wireless sensor networks," in PERCOMW 05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops, (Washington, DC, USA), pp. 146-150, IEEE Computer Society, 2005.

[27] H. Chan and A. Perrig, "Security and privacy in sensor networks," IEEE Computer Magazine, pp. 103-105, Oct. 2003.

[28] N. Gura, A. Patel, A. W, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and rsa on 8-bit cpus," pp. 1 19-132, 2004.

[29] W. Zhang, N. Subramanian, and G. Wang, ― Lightweight and compromise resilient message authentication in sensor networks,‖ in IEEE INFOCOM, Phoenix, AZ., April 15-17 2008.

[30] H. Wang, S. Sheng, 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 IEEE ICDCS, Beijing, China, 2008, pp. 11–18.

[31] Wenliang Du, Jing Deng, Yunghsiang S. Han, “A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge” in 2004.

[32] T. A. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, 1985.