ISSN No. 0976-5697

Volume 5, No. 5, May-June 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Secure Source-Based Loose RSA Encryption for Synchronization (SSOBRSAS) and Evolutionary Clustering Based Energy Estimation for Wireless Sensor Networks

V.Saravanan
Associate Professor, Department of Master of Computer Applications, Hindusthan college of arts and science, Coimbatore, Tamilnadu, India,

R.Rajkumar
Research scholar, Department of Computer Science, Hindusthan college of arts and science, Coimbatore, Tamilnadu, India,

Abstract: Designing and developing a well organized energy efficient estimation with secure based network protocol plays most important considerable responsibility in Wireless sensor networks, since of less communication energy and less availability of resources in WSN. In order to performs this process first need to evaluate the energy for each nodes in WSN and find misbehavior nodes in the WSN ,in order to hand this difficulty problem in this work initially first estimate the energy values of each nodes using evolutionary based clustering methods in the WSN .After that performs secure source based RSA encryption schema methods to identify unauthorized nodes in the WSN ,without performing communication process between one nodes to another nodes in the WSN once misbehavior nodes identified then perform key management and cryptographic process using RSA encryption. WSNs that are significantly reduce the amount of message communication desirable designed for rekeying to stay away beginning hard keys. Experimentation results measures the performance of proposed system along with energy utilization of the system under usual procedure and discover malicious nodes in wireless sensor network.

Keywords: Wireless Sensor Networks, Routing, Secure Loose Synchronization, Secure Time Synchronization for Wireless Sensor Networks, Sensor-Based Cyber-Physical Systems, cryptographic algorithm such as RSA, clustering, Expectation maximization (EM) and evolutionary clustering

I. INTRODUCTION

In wireless sensor networks, sensors nodes sends packets from one sensor node to another sensor nodes without loss of information and less resources are occupied to complete this process .These process have been carried out from source to destination nodes in the paths, where several number of building blocks have been carried in this work to send packets from source to destination in WSN. Sensor nodes are predicted intended for on-the-fly consumption and unattended form of procedure [1-5]. They are predictable to carry out dispersed logic and account to identify actions to a place of base stations connected through the sensor network. Each and every sensor nodes in the WSN is charged through restricted battery-supplied power.

In order to perform this process a several number of nodes can be posited in remote position areas, it is characteristically not sufficient to renew their power level. Once a selected node reaches it dead state or corresponds to low battery level, it is specified as dead node .So it decrease the lifetime of the entire wireless sensor network process for every protocol, it becomes sufficient to propose, energy-efficient protocols with the intention to permit sensor nodes transmit their packets from one base station to another base station in the Wireless Sensor Network (WSN).Since it need centralized authority to manage energy efficiency of the WSN designed for numerous WSN applications, In order to perform centralized authority process security based energy efficient is need to design ,to reduce loss of information and discover unauthorized nodes in the WSN . Following, since the transmission cost is the majority leading issue in a sensor’s energy utilization [6-7], in present ”chatty” schemes, several number of the energy utilization methods have been used in earlier years to overcome the problem of the energy utilization factor with the calculation of restricted safety process. From the security point of view, it becomes significant to make available authentication and accurate information to neighboring sensor nodes and in the direction to activate time-critical reaction [8]. Protocols are supposed to be presented flexible in opposition to false information introduce to WSN through harmful and unauthorized nodes. Or else, consequences designed for broadcasting unnecessary information are precious; to reduce restricted network assets.

All of the existing energy efficiency based secure synchronization protocols send packets from source to destination path divide synchronization communication and make use of position point, to perform encryption methods to make sure the security level of sensor nodes in the WSN which are protected internationally synchronized. In conventional protocols it becomes complicated to manage this process where it need as radio frequency (RF) to perform communication among nodes in the WSN with less energy consumption and do not essentially should preserve perfect synchronization for complete Sensor nodes in the WSN. In order to overcome above mentioned problems and design well organized energy efficiency based secure protocol in the WSN; in this work propose an evolutionary based expectation maximization clustering algorithm (EEMCA) to enhance the level of energy efficiency in the WSN and deal with the problem of security by using RSA in synchronization SOBOS protocols designed for WSNs.

II. BACKGROUND STUDY

Many of the existing clustering based routing protocols [9-10] recommend to broadcasting information beginning from one sensor nodes (cluster head) to cluster member based on the source nodes selected in WSN straightforwardly. This clustering based routing protocol correctly utilizes energy, during transmission process in earlier work [11] for WSN. Geographic routing [13-14] makes use of the substantial position to address the results of energy consumption through node address. By using this node address information conclude the destination address by means of seeming it beginning the position server [15], or through calculating it by means of a hash function in database scheme. In this methods generally the nodes sends a packets to nearest neighbor nodes in the network that are closest to destination nodes in the WSN. If the nodes reaches the dead states, because less energy power present in the WSN and it doesn't need to reach to the destination node in the WSN.

Constrained Shortest- Path Energy-Aware based clustering Routing Algorithm [16] is proposed in earlier work to increase network lifetime of the network in the WSN. Less consumed energy nodes are selected as cluster head within the constrained specified in the work and formation of cluster based on selected cluster head in their particular cluster. CHs establish the most excellent communication assortment for every one node and make use of a best efficient path in the WSN to conclude best routes in the WSN. If the corresponding CH nodes reach to dead state then other nodes which is similar to energy level is selected as CH. The major issues of this work doesn't our necessitate base stations to be familiar with the point of sensor nodes and challenge an impartial energy debauchery of power crossways of each and every one of nodes all the way through the life span of the network.

Similarly the other methods such as [17]–[20], we principally concerning about the false addition and unauthorized of messages starting an external malicious node; so the insider attacks are exterior to the possibility of this effort. The security results of this category of the work are named as self-motivated en-route filtering scheme in the literature work [21]. Our underlying principle designed for taking into consideration of this category of safety mechanism is with the intention of they are successful methods designed for resource-constrained strategy approximating WSNs as the malevolent information is instantaneously clean out beginning the system earlier than broadcast moreover much in the network, therefore also help out to accumulate energy . Furthermore, we presume with the intention of attacks on clocks are distinguish through the further interruption they determination initiated addicted to the network as in [22].

III.EVOLUTIONARY BASED CLUSTERING ESTIMATION FOR ENERGY EFFICIENCY WITH RSA BASED ENCRYPTION

In order to perform secure authentication based energy efficient in the network, nodes in the wireless sensor network is represented as graph $\mathrm{G(V.E)}$ Where V vetrices corresponds to the number of nodes presented in the networks and edges E represents the number of connection between one node to another nodes in the network .Two similar nodes in the network have communicate with each other by connecting edges in the networks ,let N indicate a network that corresponds to m mobile nodes, $\mathrm{N_1,..\,N_m}$ and their data items corresponds to n data items $\mathrm{d_1, d_1, \ldots .\, d_m}$.

For every one pair in the mobile nodes is represented as $\mathrm{N_i}$ and $\mathrm{N_j}$, let $\mathrm{t_{ij}}$ indicate the interruption of transmitting cost of each and every data item in the network among two nodes in the networks .In this paper SOSBRSAS protocol have been carried out by using four major steps in the network such as efficient energy estimation using evolutionary based efficient EM clustering algorithm , Time-Based Key Management (TKM), Crypto (CRYPT) using RSA algorithm, and Filtering-Forwarding-Synch (FFS) Modules.

Expectation maximization is one of the major important clustering with iterative procedure for evaluation of the energy efficiency results in cluster through the cluster head ,lowest energy utilized nodes is preferred as cluster head that alternates among expectation (E-) steps and maximization (M-) steps. The expected value to choose most favourable cluster member in the network based on E-step, it is computed in Eq. 1.The M-step follows to improve the results of network lifetime through the maximization of expected energy efficiency value is achieved to all nodes in the networks ,the original network node information are initially discovered with predefined or measuring previous past to past communication nodes in the network it is denotes as $x_1, \ldots .\, x_n$and the unobserved nodes information is represented as labels $z_1,,,,, z_n, where\ z_i = (z_{i1}, \ldots, z_{lg})$. It requires specific initialization process o perform clustering process in the network along with fuzzy membership function and maximization of energy efficient estimation results in the
network for each cluster .

$$\tilde{\mathrm{z}}_{\mathrm{ig}} = \frac{\pi_{\mathrm{g}} \emptyset \left(\mathrm{x_i} \middle| \mu_{\mathrm{g}}, \Sigma\,\mathrm{g}\right)}{\sum_{\mathrm{h}=1}^{\mathrm{c}} \pi_{\mathrm{h}} \Phi(\mathrm{x_i}|\mu_{\mathrm{h}}, \Sigma\,\mathrm{h})} \qquad (1)$$

During the E-step, we substitute z_{ig} through $\tilde{\mathrm{z}}_{\mathrm{ig}}$in Eq. 1 to obtain the accepted energy efficient results value. During the M-step, this to obtain the accepted energy efficient results value is exploiting resultant in the updates:

(2)

$$\tilde{\pi}_{\mathrm{g}} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}}}{\sum_{\mathrm{g}-1}^{\mathrm{G}} \sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}}}, \tilde{\mu}_{\mathrm{g}} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}} \mathrm{x_i}}{\sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}}} \text{ and}$$

$$\tilde{\Sigma}_{\mathrm{g}} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}} (\mathrm{x_i} - \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}} \mathrm{x_i}}{\sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}}}) (\mathrm{x_i} - \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}} \mathrm{x_i}}{\sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}}}) (\mathrm{x_i} - \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}} \mathrm{x_i}}{\sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}}}}{\sum_{\mathrm{i}=1}^{\mathrm{n}} \tilde{\mathrm{z}}_{\mathrm{ig}}}$$

In EM clustering algorithm performs based on initialization, process only it becomes implies constancy for all nodes in the cluster similarly, but it may not applicable to all the nodes in the cluster, since if the cluster size is less or high it need to change automatically .In order to overcome these problem in this work we refer evolutionary based expectation maximization clustering algorithm for cluster formation and evaluation of energy efficiency for each nodes in the network.

A. *Evolutionary algorithm with EM:*

In this algorithm where each and every step of the cluster process require difference initialization step based on the cluster size of the network, the nodes in the network for cluster formation is initiated through evolutionary algorithm in order to perform this process automatically for each cluster we additionally add two parameters into EM Algorithm one of them is mixture component $j = (1,,,,, J)$ indexes offspring, and another one of them is $k = (1,,,,. K)$ indexes parents. To perform this process in

EM algorithm based on the fitness function assigned to each and every nodes in the cluster instead of $\tilde{z}_{ig}$ use a $\hat{z}_{ig}$ is given by ,

$$F(\vartheta_j|x,\hat{z}) = \sum_{g-1}^{G}\left\{log\left(\frac{\sum_{i=1}^{n}\tilde{z}_{igj}}{\sum_{g-1}^{G}\sum_{i=1}^{n}\tilde{z}_{igj}}\right) - \frac{(\sum_{i=1}^{n}\tilde{z}_{igj})p}{2} \times log2\pi - \frac{\sum_{i=1}^{n}\tilde{z}_{igj}}{2} log\ (det\left|\frac{\sum_{i=1}^{n}\tilde{z}_{igj}(x_i-\frac{\sum_{i=1}^{n}\tilde{z}_{igj}x_i}{\sum_{i=1}^{n}\tilde{z}_{igj}})(x_i-\frac{\sum_{i=1}^{n}\tilde{z}_{igj}x_i}{\sum_{i=1}^{n}\tilde{z}_{igj}})'}{\sum_{i=1}^{n}\tilde{z}_{igj}}\right| + \sum_{i=1}^{n}\left[x_i - \frac{\sum_{i=1}^{n}\tilde{z}_{igj}x_i}{\sum_{i=1}^{n}\tilde{z}_{igj}})'\right]\left[\frac{\sum_{i=1}^{n}\tilde{z}_{igj}(x_i-\frac{\sum_{i=1}^{n}\tilde{z}_{igj}x_i}{\sum_{i=1}^{n}\tilde{z}_{igj}})(x_i-\frac{\sum_{i=1}^{n}\tilde{z}_{igj}x_i}{\sum_{i=1}^{n}\tilde{z}_{igj}})'}{\sum_{i=1}^{n}\tilde{z}_{igj}}\right] \times \left(x_i - \frac{\sum_{i=1}^{n}\tilde{z}_{igj}x_i}{\sum_{i=1}^{n}\tilde{z}_{igj}}\right)\right\} \quad (3)$$

We will describe continued existence in energy efficiency based cluster formation as the $K \in (1\ or\ 4)$ solutions for each nodes in the network . If the value of k becomes large it produces best cluster formation result in the network. Random transformation determination be produce inside the $\hat{z}_{igk}$ at every imitation phase of clustering process in the network along with two different evolutionary algorithm such as mixture evolutionary algorithm, every one of the K parents determination create $J = K$ offspring, and J determination obtain a value roughly equivalent to n. Then it added to $\hat{z}_{igk}$ for each of the nodes such that to each one of the cluster members in the nodes automatically to complete network, then secondly proposed to improve expected energy efficient results by using Z_{igk} expected values, $\hat{z}_{igk}$

$$\tilde{z}_{igk} = \frac{\pi_{gk}\emptyset(x_i|\mu_{gk},\sum g)}{\sum_{h=1}^{c}\pi_{hk}\Phi(x_i|\mu_{hk},\sum hk)} \quad \mathbf{(4)}$$

Then formed cluster performs security process by generation of key values to all nodes in the network using local time and it is known as Time-Based Key Management module. When source nodes send a packets to destination through the key values generated to each nodes along with time , the keys are a purpose of the present restricted time value (t_1) and moreover an initialization vector (IV) or previous key K_{j-1} as,

$$K_1^t = F(t_1, IV) \qquad K_j^t = (t_1, K_{j-1}), \quad (5)$$
$$F=G(Dif,R_{e/h}),$$

Where G is a function of $R_{e/h}$ and D_{if}. $R_{e/h}$ is the operation of moreover encryption D_{if} is the diffuser. The principle of D_{if} is to disseminate the bits of XOR ed t_1 and k_{j-1} with s-bit left round shift operation earlier than $R_{e/h}$ as follows:

$$D_{if} = (K_{j-1} \oplus t_1) << s. \quad (6)$$

The amount of shift, s, is determined by,

$$s = l * n + n \quad n = 0,1,..,log_2 Size(K) - 1 \quad (7)$$

Where B and l indicate the desired key size and the size of the timer bits. In essence, both D_{if} and $R_{e/h}$ in F are principally make use of to enlarge the unpredictability of bits in the key, K for malicious entities. It is probable to propose $R_{e/h}$ by means of stream ciphers with φ Euler's totient function .

Time-Based Key Management Algorithm 2:

Technique used: RSA Cryptographic Technique

Steps:

a. Source node sends data to sink
b. Using local clock value as a key
c. Key= Current local time value+ Initialization vector
d. Encryption Operation using RSA algorithm
e. Dynamic Key generation

Algorithm 2:

a. S send data to sink //S-Source node
b. Generate key using current local time value (t_l) and initialization vector(IV)
c. Generation of key $K_1^t = F(t_1, IV)$ $K_j^t = (t_1, K_{j-1})$,
d. Generate function $F = G(Dif, R_{\frac{e}{h}})$
e. For $R_{e/h}$ operation using RSA cryptographic function

\\ Inside RSA consists of two parts

f. Key Scheduling Algorithm (KSA)
g. Pseudo-Random Generation Algorithm (PRGA)
h. Variable Size Key (K) Turns an Array (S) of Identity Permutation into a 'Random' Permutation
i. The Size of the Key $K = 1\ to\ 256$ Bits
j. The Size of the Array $N = 256$ Bytes
k. Use the same secret key as during the encryption phase.
l. Generate key stream by running the KSA and PRGA
m. XOR key stream with the encrypted text to generate the plain text

Then process perform security based encryption process to remove malicious node activities in the network through the key values generated from RSA algorithm with TKM module .It simultaneously check the private key and public key of each node in the network and it is verified in above mentioned TKM module, if the particular nodes works well the data or packets transmitted to that nodes or else it is considered as malicious node in the network. Initially the original packets are forwarded to source nodes without consideration of key values and then checks secutiy usng RSA ,then perform reencryption if any one of the nodes is considered as malicious node in the network along with data delivery path in cluster ,it procedure as follows .

Crypto Module Algorithm 3

Technique used: RSA algorithm

Steps:

a. Obtains the dynamic key from the Time-Based Key Management
b. Verify the key
c. Incorporate RSA algorithm for encryption
d. Classify the incoming packet as malicious

Algorithm 3:

a. Get dynamic key from TKM module
b. Verify the dynamic key
c. If key value is not correct then
d. New key is obtained
e. Else
f. Process the encryption algorithm

```
    // RSA algorithm consists of two steps
   //1.Key Scheduling algorithm
g.  State array generation
h.  Input($S, K$)
i.  for($i = 0 \ to \ N - 1$)
j.  $S[i] = i$
k.  $j = 0$
l.  for($i = 0 \ to \ N - 1$)
m.  $j = j + k[I \ mod \ l] + S[i]) \ mod \ N$
n.  $\varphi(i) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$
o.  Swap ($S[i], S[j]$)
// 2. Pseudo-random generation algorithm
p.  Input($S$)
q.  $i = 0$
r.  $j = 0$
s.  $i = i + 1$
t.  $j = (j + S[i]) \bmod N$
u.  Swap ($S[i], S[j]$)
v.  $L = (S[i] + S[j]) \bmod N$
w.  Output $S[L]$
x.  For Decryption use same secret key
y.  Generate key stream by running the KSA and
    PRGA
z.  XOR key stream with the encrypted text to
    generate the plain text
```

In order to generate key values automatically for all nodes in the network using RSA algorithm and it procedure as follows RSA stands for Rivest, Shamir and Adleman. It is one of the commonly used encryption algorithm in several work, it used s variable size of data blocks to generate key values to each node in the network encryption. The key-pair (p, q) is generated from variable n, by multiplication of those prime numbers, where p and q are prime numbers (p, q) RSA has been expansively second-hand for institute protected communication channels among all paths in the cluster and for verification the individuality of results insecure communication medium.RSA absorbs a public key and a private key. The public key can be eminent to one and all and it is second-hand designed for encrypting original packet information in the nodes during communication process. the corresponding packets data are encrypted with the public key can only be decrypted in a correct destination node using the private key. The keys for the RSA algorithm are generated the following way:

Algorithm 4 : RSA algorithm

a. Choose two distinct prime numbers p and q for each nodes in the network
b. Compute $\mathrm{n} = \mathrm{pq}$. n is used as the modulus for both the public and private keys, the length of each key is expressed using bit length B.
c. Compute $\varphi(\mathrm{n}) = \varphi(\mathrm{p})\varphi(\mathrm{q}) = (\mathrm{p} - 1)(\mathrm{q} - 1)$, where φEuler's totient function is.
d. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(\mathrm{e}, \varphi(\mathrm{n})) = 1$; i.e. e and $\varphi(\mathrm{n})$ are coprime. e is released as the public key exponent.
e. Determine d as $\mathrm{d} - 1 \equiv \mathrm{e} \ (\mathrm{mod} \ \varphi(\mathrm{n}))$, i.e., d is the multiplicative inverse of e (modulo φ(n)).
   a) This is more clearly stated as solve for d given $\mathrm{de} \equiv 1 \ (\mathrm{mod} \ \varphi(\mathrm{n}))$
   b) d is kept as the private key exponent.

IV.EXPERIMENTATION RESULTS

In this section we analysis the results of secure energy efficiency based evolutionary clustering algorithm and RSA based encryption for security in SOBOS protocol ,it is named as enhanced SOSBRSAS results ,it can be compared to existing SOBOS protocol via usages of network simulator tool such as ns2 to analysis results . First, simulation results are obtainable to check the result of evolutionary based clustering algorithm for energy efficiency under standard process and second, the collision of the $selective - reEnc$ procedure in the WSN is well considered using RSA algorithm in each cluster. Third, filter out the insider malicious node attacker in each cluster. In conclusion, finally compare these results into other existing SOBOS algorithm .The experimentation results of proposed and existing results is analyzed using the parameters like packet delivery ratio, computation cost of each methods and detection accuracy of malicious node in the networks.

A. packet Delivery Ratio:

Packet delivery ratio is defined as relationship between the number of packets which correctly delivered from source to destination path in the network and total number of packets sended by user. This illustration is represented as, $\sum$ Number of packet receive / $\sum$ Number of packet send

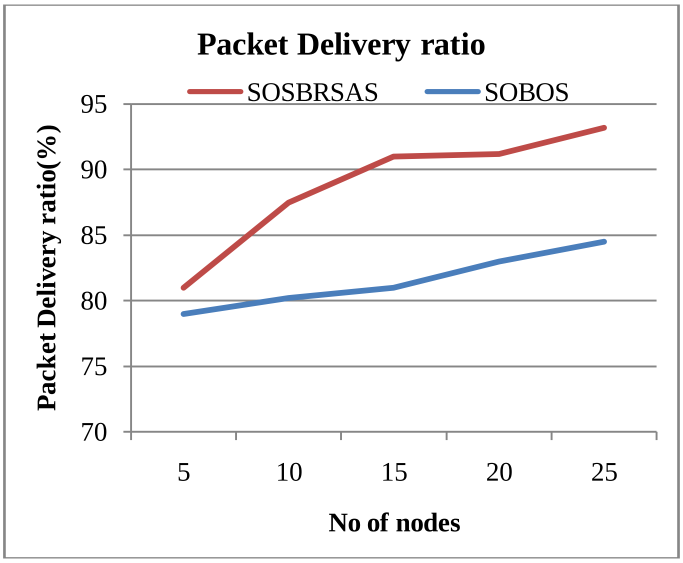

Figure 1: Packet Delivery Ratio

The Packet delivery ratio is shown in figure 1. In the X-axis number of nodes is taken. A y-axis packet delivery ratio result is analyzed between SOBOS and proposed **SOSBRSAS** encryption. These results obviously show with the intention of, if the number of nodes is increases the packet delivery ratio is reduce in existing and proposed methods. The packet delivery ratio of the proposed system is high because of encryption algorithm with fewer attackers.

B. Computation Cost:

Computation cost of the existing and proposed system is defined as how the algorithm takes time to complete entire process, in this work we analysis the time completion time of RC64 algorithm and RSA algorithm for encryption, decryption re-encrypting of packets by the side of each hop in the network

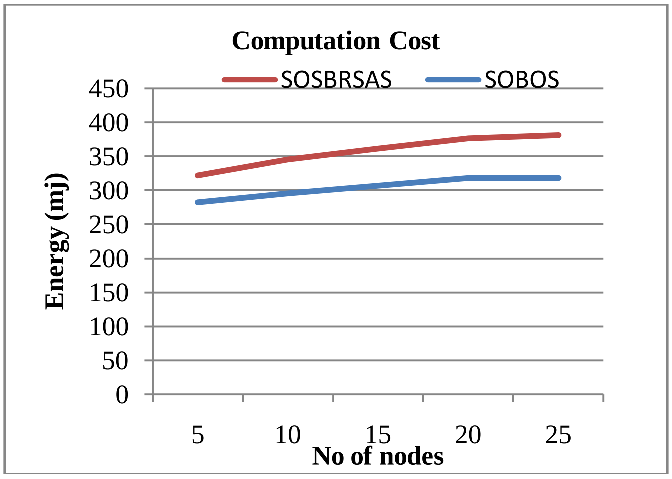

Figure 2: Communication cost

The Computation cost is shown in this Figure 2. In the X-axis number of nodes is taken. Y-axis computation cost of SOBOS and proposed SOSBRSAS encryption is analyzed. This graph clearly shows that if the number of nodes is increases the computation cost is increases in existing methods when compare to proposed SOSBRSAS, the computation cost is decreases.

C. Detection Accuracy:

Detection accuracy is defined as how well the systems distinguish the malevolent nodes in the WSN.

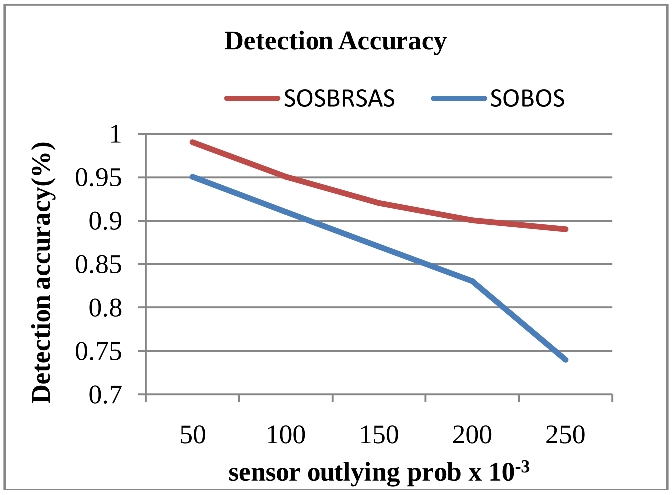

Figure 3: Detection accuracy

The detection accuracy is shown in this Figure 3. In the X-axis number of nodes is taken. Y-axis detection accuracy of SOBOS and proposed SOSBRSAS encryption is analyzed. This graph clearly shows that if the number of nodes is increases there is less detection accuracy. But in the SOSBRSAS insider attack detection method, there is more detection accuracy when compare to SOBOS.

V. CONCLUSION

In this work proposed efficient energy efficiency based base secure time synchronization approach for wireless sensor nodes in the network through the estimation of energy values of each and every nodes in the network by using evolutionary based clustering algorithm. Then perform secure encryption through usage of RSA algorithm generate key values to each nodes in the cluster in order to transmission of packets from source to destination path in correct manner without loss of information or packets in the nodes, it limits resource-constraints of each nodes in the cluster and finally focal point on the fact that the communication cost is important in WSNs,. It reduces communication cost and increases network lifetime through the evaluation of energy efficiency for each nodes in the cluster by using evolutionary based EM clustering algorithm with more security operations. By make use of the RSA algorithm the misbehavior nodes are monitored continuously and remove /filter those nodes in the cluster, improves packet delivery ratio, high detection accuracy and a less energy consumption

VI. REFERENCES

[1]. C. M. Okino and M.G. Corr.” Statistically Accurate Sensor Networking “ *Wireless Communications and Networking Conference*, 2002

[2]. G.J. Pottie ,” Wireless sensor networks*”,Information Theory Workshop*, pages 139.140, 1998.

[3]. J. Agre and L. Clare ,”An integrated architecture for cooperative sensing networks”, *Computer*, 33(5):106.108, 2000

[4]. R. Min, M. Bhardwaj, Seong-Hwan Cho, E. Shih, A. Sinha, A. Wang and A. Chandrakasan ,”Low-power wireless sensor networks”, *Fourteenth International Conference on VLSI Design*, pages 205.210, 2001.

[5]. S. Lindsey and C. Raghavendra ,” PEGASIS: Power-Efficient Gathering in Sensor Information Systems ,” *Intl. Conf. on Communications*, 2001.

[6]. H. Hou, C. Corbett, Y. Li, and R. Beyah, “Dynamic energy-based encoding and filtering in sensor networks,” *in Proc. of the IEEE MILCOM*, October 2007.

[7]. A. Uluagac, R. Beyah, Y. Li, and J. Copeland, “Vebek: Virtual energy based encryption and keying for wireless sensor networks,” *Mobile Computing, IEEE Transactions on*, vol. 9, no. 7, pp. 994 –1007, july 2010

[8]. S. Uluagac, C. Lee, R. Beyah, and J. Copeland, “Designing Secure Protocols for Wireless Sensor Networks,” *Wireless Algorithms, Systems, and Applications*, vol. 5258, pp. 503-514, Springer, 2008.

[9]. A. Manjeshwar and D.P. Agrawal ,“TEEN: a routing protocol for enhanced efficiency in wireless sensor networks,”*Intl. Proc. of 15th Parallel and Distributed Processing Symp.*, pages 2009.2015, 2001.

[10]. W.R. Heinzelman, A. Chandrakasan and H. Balakrishnan,” Energy efficient communication protocol for wireless micro sensor networks”, *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, pages 3005.3014, 2000.

[11]. G.J. Pottie and W.J. Kaiser ,” Wireless integrated network sensors”, *Communications of the ACM*, 43(5):51 . 58, 2000.

[12]. J. Gao, L. J. Guibas, J. Hershberger, L. Zhang, and A. Zhu ,” Geometric spanners for routing in mobile networks “, *IEEE Journal on Selected Areas in Communications*, 2005, 23.174–185.

[13]. S. Lee, B. Bhattacharjee, and S. Banerjee ,” Efficient geographic routing in multihop wireless networks”, *In IEEE/ACM MOBIHOC*, 2005, pp. 230–24

[14]. J. Li, J. Jannotti, D. DeCouto, D. Karger, and R. Morris,” A scalable location service for geographic ad-hoc routing”, *In IEEE/ACM MOBICOM*, 2000, pp. 120–130

[15]. S. Ratnasamy, B. Karp, L. Yin, F. Yu, D. Estrin, R. Govindan, and S. Shenker ,” GHT: a geographic hash table for data-centric storage”, *In ACM WSNA*, 2002, pp. 78–87.

[16]. M.A. Youssef, M.F. Younis and K.A. Arisha ,”A Constrained Shortest- Path Energy-Aware Routing Algorithm for Wireless Sensor Networks “, *Wireless*

Commun. and Networking Conference, 2002, 2:794.799, 2002

[17]. Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," *Proc. of IEEE INFOCOM*, pp. 1–12, April 2006.

[18]. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE JSAC*, vol. 23, no. 4, pp. 839–850, April 2005.

[19]. C. Kraub, M. Schneider, K. Bayarou, and C. Eckert, "Stef: A secure ticket-based en-route filtering scheme for wireless sensor networks," *The 2nd Int. Conf. on Availability, Reliability and Security (ARES)*, pp. 310– 317, April 2007.

[20]. Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Comput. Commun., vol. 30*, no. 11-12, pp. 2314–2341, 2007.

[21]. S. Ganeriwal, S. ˇCapkun, C.-C. Han, and M. B. Srivastava, "Secure time synchronization service for sensor networks," *in Proc. of the ACM workshop on Wireless security (WiSe)*, 2005, pp. 97–106

[22]. H. Song, S. Zhu, and G. Cao, "Attack-resilient time synchronization for wireless sensor networks," *Ad Hoc Networks*, vol. 5, pp. 112–125, 2005.