Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.244 – 254

RESEARCH ARTICLE

Self-optimization and Self-Protection (Transactional Security) in AODV Based Wireless Sensor Network

[1]Rajani Narayan, [2]Dr. B.P. Mallikarjunaswamy, [3]M.C. Supriya

[1]Research scholar, Department of Computer Science and Engineering, Jnanasahyadri, Kuvempu University, Shankaraghatta, Shimoga, Karnataka, India

[1]Associate Professor, Department of MCA, RNS Institute of Technology, Bangalore

[2]Professor, Dept. of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

[3]Research scholar, Department of Computer Science and Engineering, Jnanasahyadri, Kuvempu University, Shankaraghatta, Shimoga, Karnataka, India

Abstract— WSN technologies present significant potential in several application domains. Given the diverse nature of these domains, it is essential that WSNs perform in a reliable and robust fashion. This paper presents methods of integration of autonomic computing principles into WSNs. PSO based clustering for self-optimization and watch mechanism based method for self-protection from black hole attack has been presented in this paper, the paper proposes a novel approach for transactional security with chaos based AES cryptography. Results show that lifetime and throughput of wireless sensor network can be increased using this methods.

Index Terms—WSN; Self-Optimization; Self-Protection; PSO; Hierarchical Clustering; Black hole Attack

I. INTRODUCTION

Developed with an initial motive to serve military services WSNs have now been started to find applications in health, traffic and many consumer as well as industrial applications. Wireless Sensor Network is a group of densely situated sensors nodes deployed in a solitary environment with a purpose of sensing, monitoring and computing.

Wireless sensor networks are normally used in adverse conditions with no human existence and therefore, they must be tolerant to situations like network failure. Hence nodes in WSNs should be smart to recover from breakdown with minimum human contribution. Networks must be adaptable to autonomous configuration of parameters to recover from failure. Application of autonomic computing in wireless sensor network can lead to establishment self-configuration characteristics in WSNs.

The concept of autonomic computing was given by IBM in 2001 for elimination of human efforts in managing today's computer systems [1]. Autonomic computing refers to self-managing property of a system through which systems can manage themselves according to high level objectives provided by the administrator [2].

In general Autonomic computing systems reveal following important characteristics:

- *Self Awareness*: An autonomic system knows itself, its states and its behavior.
- *Self Configuration*: An autonomic computing system should be able to configure itself in changing and unpredictable conditions.
- *Self Optimization*: An autonomic system should be able to perceive optimal behavior and optimize itself to improve its performance.
- *Self Healing*: An autonomic system should be able to sense and recover from possible problems and continue to function smoothly.
- *Self Protection*: An autonomic system should be able to sense and defend its resources from domestic and outside attacks and to preserve overall system security and integrity.
- *Background Aware*: An autonomic computing system must be aware of its working context and should be capable of reacting on changes.
- *Flexibility*: An autonomic computing system must be able to work in open and extensible environment and should be flexible to hardware and software architectures.

The application of autonomic computing is major area of interest from last decade. In [3] Radu et al presented policy based generic autonomic architecture and a four step method for effective development of self-managing system. In [4] the application of autonomic computing to improve the performance of wireless sensor network has been presented by G.M.P. O'Hare et al. A novel data dissemination algorithm for wireless sensor networks based on trajectory-based forwarding and energy mapping has been presented in [5]. In [6] concept of autonomic sensor element has been presented to provide advantage of autonomic computing in WSNs. The main problem in WSNs is limited battery capacity of the system; hence resources must be used in efficient manner so that optimal performance can be obtained from network. Based on this idea Tynan et al presented concept of opportunistic hibernation to increase the network lifetime [7]. Adaptable mobile agent based data dissemination protocol to add autonomic features to WSNs have been proposed by Igor M. B. Spadoni et al [9]. In [10] self optimization of WSNs based on ant colony optimization has been presented. Energy level, delay and velocity based ant colony optimization provides optimal routing and improves the performance of WSNs.

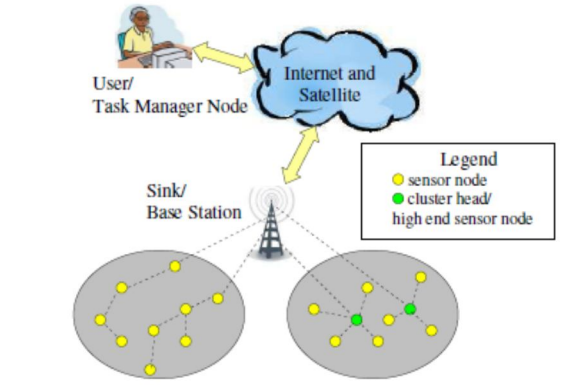
Rest of this paper is organized as follows: Section II presents overview of WSNs. Section III describes, Section IV describes, Section V describes, Section VI describes.

II. WIRELESS SENSOR NETWORK

A wireless sensor network is the accumulation of sensor nodes deployed over globe to investigate physical parameters like humidity, temperature, seismic events, vibrations etc. Since the scope of WSN is so broad, there is a considerable variation in hardware/software solution space of WSN technology. A simplified view of hardware/software helps develop a basic understanding of how these systems work. Most WSNs are multi-hop networks and rely on a communication stack that includes Media Access Control (MAC), routing and transport layers. There are many protocols for each of these layers, but they are not the same protocols found in wired networks or even Wi-Fi networks.

The WSN was initially coined for military and heavy industrial applications in around 1950s. A Sound Surveillance System (SOSUS) was the first network developed by US Military forces to track Russian submarines. This network used submerged acoustic sensors – hydrophones – distributed in the Atlantic and Pacific oceans. 1960s-70s was the period of internet exploration which we see today.

The Distributed Sensor Network program (1980) was launched by US Defence Advanced Research Projects Agency (DARPA) to explore the challenges in the implementation of sensor networks. The idea of distributed sensor networks was initially made with an assumption that several tiny devices called nodes team-up with each other to deliver the information which was routed to them based on best availability. Both academic and industry predicted the potential of this field and made joint venture to solve the difficulty in this type of systems. Several examples include UCLA Wireless Integrated Network Sensors University of California at Berkeley Pico Radio program (1999), NASA Sensor Zig Bee Alliance (2002) etc. WSN's have drawn a huge interest since 1998, in this new trend of research networking capability and network information handling were the prime area of research. A wireless sensor network is collection of large number of sensor nodes with sensing, communication and computing capabilities. The sensor nodes are distributed in a hostile environment to gather data about physical characteristic of the field. The collected by these sensor nodes can be collected a base station or several sink nodes linked to the network. The operation of WSN has been shown in fig.1. The sensor nodes can either form a flat network topology or a hierarchical network topology [13].



(a) Flat sensor network (b) Clustered Sensor Network

Fig1: Wireless Sensor Network Operation

III. AUTONOMIC WSN

IBM proposed an automatic computing method to transfer the burden of humans to managing computer systems [13]. At the high complex levels the computers are organized to manage themselves. This could only be achieved only by making the machines capable enough to take decisions with respect to self-healing, self-protection, configuration and optimization, and feeding them with enough raw data to the machines.

The computer systems are deployed in wireless sensor networks as they are hard to manage with human efforts. In the large networks of WSN the management of nodes experience severe effects of environmental vulnerabilities, complex processing mechanisms and results in unreliable and lacking robustness. Administration with computer application would greatly benefit with their inherent automation methods in the implementation of sensor networks [14].

Intelligent agents [15] proposed one of the core technologies to enable autonomic computing. A class of software was entirely capable of displaying goal-directed, cooperative and autonomous behavior in response to external stimuli. The mechanism was composed of sense-deliberate-act cycle, which maps well onto WSNs whereas the sensor nodes sample the data to use as input in decision making process.

The contribution of autonomic computing to WSNs can be explained by following scenarios in which a common WSN problem in WSN operation can be tackled using autonomic principles.

- It is assumed that nodes constituting the network can never be perfectly positioned. Hence self configuring nodes are setup and the gap in WSN can be evaluated either by sensing or networking viewpoint. [16] Provides an example of this, a protocol for automatically building a network out of randomly distributed nodes.
- Self-protection attribute monitors voltage levels remotely or locally so that the agent can avoid being lost n any manner.
- The ability to repair damage to the network is called self healing. The harsher conditions results to energy depletion and incidental damage. A gradual degradation of network, network path break and gaps appear in sensing coverage area. The WSN requires to self-heal itself and repair the damaged area. Renegotiating network routes, activation of redundant nodes and informing a higher authority are some of the methods in to minimize loss in this context.
- Maximum efficiency is a necessary factor in WSN. The self-optimization technique is an important trait against this. A low bound quality of service can be provided by re-enabling the redundant sensor nodes that go to low power sleep mode and results in same accuracy and service quality. This reduces the energy consumption of the network to a great extent [[17].

IV. AD-HOC ON DEMAND DISTANT VECTOR ROUTING PROTOCOL

The Ad hoc On-Demand Distance Vector (AODV) [5] procedure allows self-starting, dynamic, multi-hop routing between contributing mobile nodes demanding to launch and uphold an ad hoc network.

AODV permits mobile nodes to find paths rapidly for novel destinations, and does not necessitate nodes to preserve paths to destinations that are not in dynamic communication. It also permits the mobile nodes to reply to link changes and breakages in network topology in a timely mode. The procedure of AODV is loop-free, by means of keeping away the Bellman-Ford "counting to infinity" problem offers rapid convergence as any change is encountered in the ad hoc network topology (normally, when a node moves in the network). Whenever a break is detected, AODV noticed the affected set of nodes in order to separate them from rout formation by utilizing the lost link.

AODV has a specific feature, it use a destination sequence number for all route entry, destination sequence number is generated by the destination to be involved along with any route data it sends to requesting nodes. The purpose of this sequence numbering is to confirms the loop freedom and is modest to program. For instance consider two routes to a destination, the requesting node is mandatory to pick the one with the highest sequence number.

Route Errors (RERRs), Route Replies (RREPs) and Route Requests (RREQs) are the message categories explained by AODV. These types of message are received through UDP, and normal IP header processing applies. For example let us consider a requesting node is likely to use its IP address as the Originator IP address for the messages. The IP limited broadcast address (255.255.255.255) is used to broadcast the message. By this we can conclude that such messages are not carelessly forwarded. But, AODV process does need certain messages (e.g., RREQ) to be spread widely, possibly throughout the ad hoc network. The variety of dissemination of such RREQs is demonstrated by the TTL in the IP header. Fragmentation is normally not needed.

As long as the terminating points of a communication assembly have lawful routes to each other, AODV does not play any role. When a path to a novel destination is required, the node broadcasts a RREQ to discover a path to the destination.

A route is obtained as the RREQ touches either the destination itself or with the help of an intermediate node with a 'fresh enough' route to the destination. A 'fresh enough' route is a lawful route entry for the destination whose related sequence number is at least as large as that comprised in the RREQ. The route is made accessible by unicasting a RREP again to the origination of the RREQ. Each of the node present in the communication field receive the request caches a route back to the creator of the request, so that the RREP can be unicast from the destination along a path to that originator, or likewise from any intermediate node that is able to satisfy the request.

Nodes that are monitoring the link conditions of next hops in termed as active routes. The RERR message is used to alert other nodes as any break is encountered in an active route. The RERR message specifies those possibly subnets (destinations) which are no longer accessible by way of the broken link. In order to permit this reporting mechanism, each node hold onto a "precursor list", encompassing the IP address for each its friends that are expected to use it as a next hop in the direction of each destination. The data in the precursor lists is effortlessly acquired in the course of the processing for generation of a RREP message, which by definition has to be delivered to a node in a precursor list. If the RREP carries a nonzero prefix period, then the originator of the RREQ which solicited the RREP information is comprised among the precursors for the subnet route.

AODV is a routing protocol, and it agreements with route table administration. Route table data should be reserved even for short-lived routes, such as are produced to temporarily store reverse paths towards nodes originating RREQs. AODV utilizes the subsequent fields with each route table entry:

A. Destination IP Address

B. Destination Sequence Number

C. Valid Destination Sequence Number flag

D. Other state and routing flags (e.g., valid, invalid, repairable, being repaired)

E. Network Interface Hop Count (number of hops needed to reach destination)

F. Next Hop

G. List of Precursors

H. Lifetime (expiration or deletion time of the route)

V. SELF OPTIMIZATION IN AODV BASED WSN

Wireless Sensor Network has witnessed increasing demand in several applications such as environmental monitoring, military field surveillance, forest fire detection and many more. These applications require deployment of several small sensor nodes in hostile environment to constantly monitor numerous parameters like temperature, pressure etc. These sensor modes transmit sensing information to a central administrator called base station. Due to densely situated nodes and hostile nature of environment it is difficult to recharge node batteries. Hence energy efficiency is prime concern in designing a WSN. In some applications it is not necessary to transmit all the sensed information to the base station instead mutual information of different nodes is used to calculate aggregate information which is then transmitted to the observer. This aggregation of data reduces overhead in network and saves significant amount of energy as well. Clustering is a method in which network is partitioned into several number of small groups called cluster, each cluster has a cluster head (central coordinator) and number of participant nodes. Clustering is a hierarchical approach, in which cluster head is tier-1 member while participant nodes are tier-2 members.

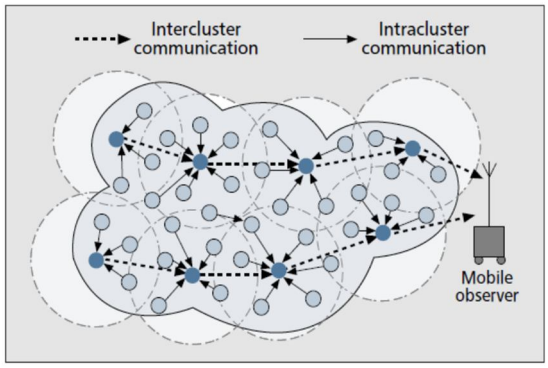


Fig2: Data flow in clustered Network

Member nodes transmit their information to cluster head and cluster head performs aggregation operation and send this information to base station. Due to continual process of aggregation and transmission cluster head looses more energy compared to participating nodes. Hence re-clustering is required periodically to select cluster heads with maximum residual energy. Optimal clustering may improve network lifetime and results in better network performance under the condition of high loads.
Consider a wireless sensor network with different amount of initial energy [11]. We present the energy model and particle swarm optimization based optimal clustering to improve network lifetime. According to heterogeneous clustering model presented in [11] assume that a fraction of population of sensor nodes is equipped with more energy resources than the rest of the nodes.

Let *m* be the fraction of the total number of nodes *n*, which is equipped with α times more energy than the others. We refer to these powerful nodes as advanced nodes, and the rest(1-m)×n as normal nodes. We assume that all nodes are distributed uniformly over the sensor field.

Consider the case of hierarchical clustering in WSN using Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. According to LEACH, load balancing and distribution between the nodes is done by re-establishment of clusters in each round. Each participating node in cluster is accountable only to its nearest cluster-head and only cluster-head is responsible to report to the base station. This process requires a large amount of energy and hence by periodic clustering each node will become cluster head. In iterative process for each round optimal percentage P_{opt} of nodes which will become cluster-heads is calculated. Assuming $1/P_{opt} P_{opt}$ as number of cycles of network, LEACH ensures that every node will become cluster-head one time after every $1/P_{opt}$ cycle. Initially P_{opt} is the probability with which each node in the network can be a cluster head. At an average number of nodes that must be selected to become cluster head per cycle per epochs is $n \times P_{opt}$. Currently elected nodes cannot be elected as cluster head in same epoch and non-elected nodes forms a set G to maintain uniform number of cluster heads. At the beginning of every cycle each node chose a random number between [0, 1] and based on this number if it is less than a threshold T(s) then the node becomes cluster head during current cycle.

The threshold is given as

$$T(s) = \begin{cases} \frac{P_{opt}}{1-P_{opt}\cdot\left(\mathrm{r} \bmod \frac{1}{P_{opt}}\right)} & if\ s \in G \\ 0 & otherwise \end{cases} \qquad (1)$$

r being number of current cycle (initially 0). The probability of election of a node as cluster head increases per cycle per epoch and becomes 1 in last cycle of same epoch.
We will calculate optimal percentage P_{opt} according to particle swarm optimization and optimized value is used for election of cluster head.

VI. Self Protection in AODV based Wireless Sensor Network

WSN has been used for surveillance and military applications operating in hostile environments, it is necessary to provide certain level of protection or fault tolerance to the sensor network so that it can resist the attacks from outsides. In WSNs, sensors can be put in non-active status to save energy, and only active sensors perform the sensing tasks. Obviously, the denser and more active the sensors are, the better the protection for the objects or the better fault tolerance for the network [12].
Internal Black hole attack from cooperative malicious nodes has been simulated in this paper. In internal black hole attack a malicious node becomes a part of the route between source and destination and after getting a chance this malicious node becomes

an active data element. This Malicious node is now starts to attack the network by transmitting the data. The WSNs are more susceptible to internal attacks because it is too difficult to detect misbehaving node.

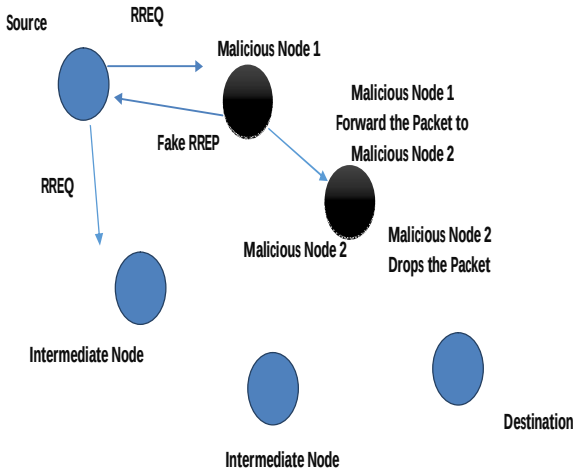


Fig3: Black-hole Detection

Watch Mechanism for black hole detection: In Watch mechanism, each node keeps two extra tables, one is known as pending packet table and another one is knows as node rating table. There are four fields in pending packet table, Packet ID, Next Hop, Expiry Time and Packet Destination.

Table I. Pending packet table

Current Node Address	Packet Drops	Packet Forwards	Misbehave

- Packet ID: ID of packet sent.
- Next Hop: Address of next hop node
- Expiry Time: Time-to-live of packet
- Packet Destination: Address of destination node.

There are also four fields in node rating table, Node Address, Packet drops, Packet forwards and Misbehave. This table updated corresponding to pending packet.

Table II. Node rating table

Current Node Address	Packet Drops	Packet Forwards	Misbehave

- Node Address: Address of next hop node.
- Packet Drops: Counter for counting the dropped packet.
- Packet Forwards: Counter for counting the forwarded packet.
- Misbehave: It has two values 0 and 1, 0 for well behaving node, 1 for misbehaving node.

In pending packet table, each node maintains track of the packets, it sent. It contains a unique packet ID, the address of the next hop to which the packet was forwarded, address of the destination node, and an expiry time after which a still-existing packet in the buffer is considered not forwarder by the next hop.

In node rating table, each node maintains rating of nodes, which are next to it (means nodes are within its communication range). This table includes the node address, a counter of dropped packets noticed at this node and a counter of successfully forwarded packets by this node.

The fourth field of the above node rating table is calculated by the ratio of dropped packets and successfully forwarded packets, if this ratio is greater than a given threshold value then this node misbehave value will be 1 (means it is interpreted as a misbehaving node), otherwise it is deliberated as a legitimate node. An expired packet in the pending packet table causes the packet drops counter to increase for the next hop correlated with the pending packet table entry. Each node listens to packets that are inside its communication range, and only to packets associated to its domain. Then, it checks each packet and prevent forged packet. If it notices a data packet in its pending packet table, then it deletes this data packet from pending packet table after authenticating the packet. If it notices a data packet that exits in its pending packet table with source address different from the forwarding node address, then it increases the packet forwarding value in node rating table.

For determining whether a node is misbehaving or act as a legitimate one, rest on the selection of threshold value. For example if we assume a threshold value of 0.5. This means that as long as a misbehaving node is transmitting twice packets as it drops it will not be distinguish. If we assume a lower value of threshold then it will increase the percentages of false positives. After finding a misbehaving node, a node will attempt to do local repair for all routes passing through this misbehaving node. If local repair process fails, then it will not transmit any RERR packet upstream in the network. This process attempts to prevent a misbehaving node from dropping packets, and also prevent blackmailing of legitimate nodes. To avoid constructing routes, which traverse misbehaving nodes, nodes drop all RREP messages arriving from nodes currently marked as misbehaving. To stop misbehaving node to act actively in a network, the all packet starting from this node has been dropped as a form of punishment.

VII. TRANSACTIONAL SECURITY IN AODV BASED WSN

Encryption has an important role in data protection for WSN. The importance of encryption realized with increasing communication. Encryption makes sense when data packets using open channels, which they can be reached by other devices or people, to transfer their contents. An Encryption system contains set of transformations that convert plain text into cipher text. In the block cipher system, plain text converts into blocks that cipher algorithm applies on them to create cipher text. The block cipher systems divided into two general principles: Diffusion and Confusion.

In Diffusion principle, each bit of plain text converts into many bits. However, in Confusion principle, number of bits doesn't change and only transformations apply to plain text, hence in Confusion principle, size of plain text and cipher text is equal. Usually both principle uses round repetition to create cipher text. Cipher algorithms have the two general categories: Private Key algorithms and public key algorithms. Private Key algorithms using single key to encrypt plain text and decrypt cipher text in sender and receiver side. Private Key algorithm samples are: DES, 3DES and Advanced Encryption Standard (AES). Public Key algorithms, such as the Rivest-Shamir-Adleman (RSA), using two different key for encrypt plain text and decrypt cipher text in sender and receiver sides. Block cipher systems depend on the S-Boxes, which are fixed and no relation with a cipher key. So only changeable parameter is cipher key. Since the only nonlinear component of AES is S-Boxes, they are an important source of cryptographic strength. So we develop a chaos S-box based AES system to provide transactional security to AODV based WSN system.

Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and a U.S. government standard for secure and classified data encryption and decryption. AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits. A data block to be encrypted by AES is split into an array of bytes, and each encryption operation is byte oriented. AES's round function consists of four layers. In the first layer, an 8x8 S-box is applied to each byte. The second and third layers are linear mixing layers in which the rows of the array are shifted, and the columns are mixed. In the fourth layer, sub-key bytes are XORed into each byte of the array. In the last round, the column mixing is omitted. So, the algorithm consists of four main steps: a substitution step, a shift row step, a mix column step and a sub-key addition step. The substitution step consists of S-boxes. The shift row step consists of cyclic shifting of the bytes within the rows. The key addition is a straight forward XOR operation between the data and the key.

VIII. RESULT

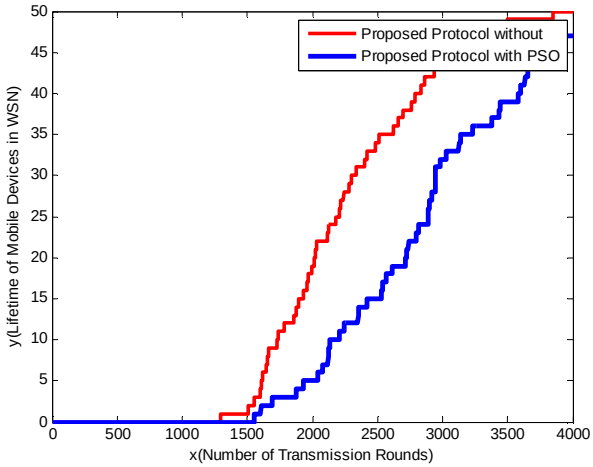


Fig5.a: Lifetime of WSN

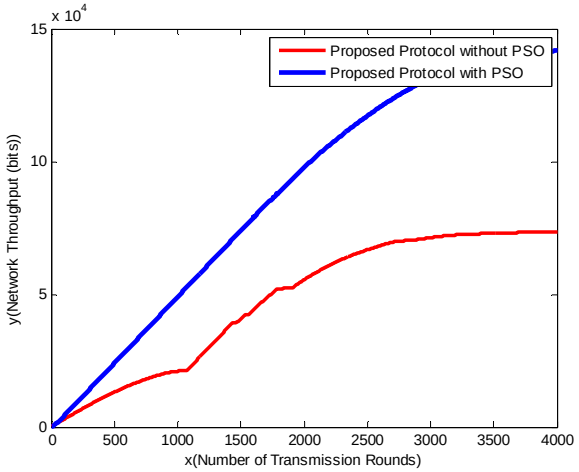


Fig5.b: Network Throughput

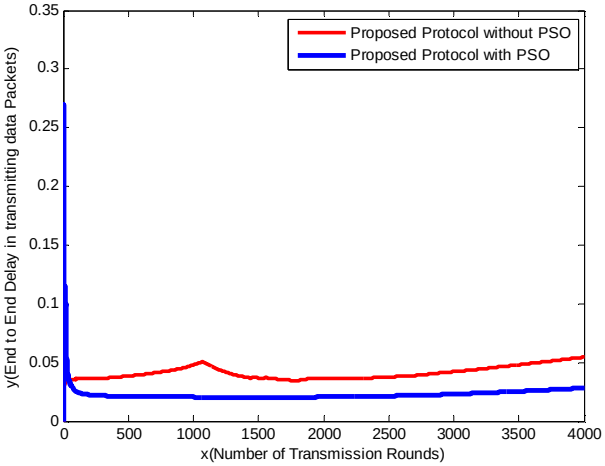


Fig5.c: End to End Delay In transmission data packets

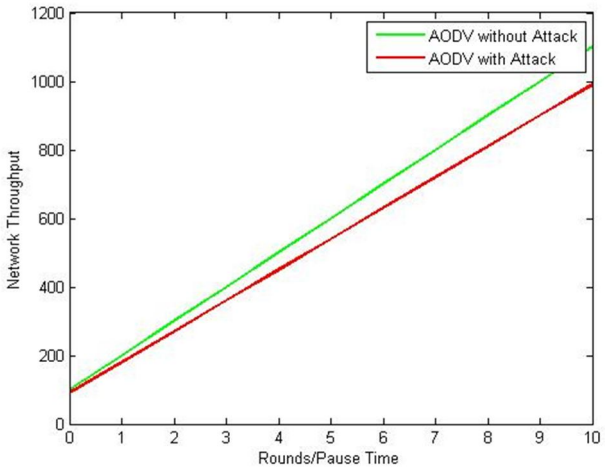


Fig5.d: Network Throughput In case of attack

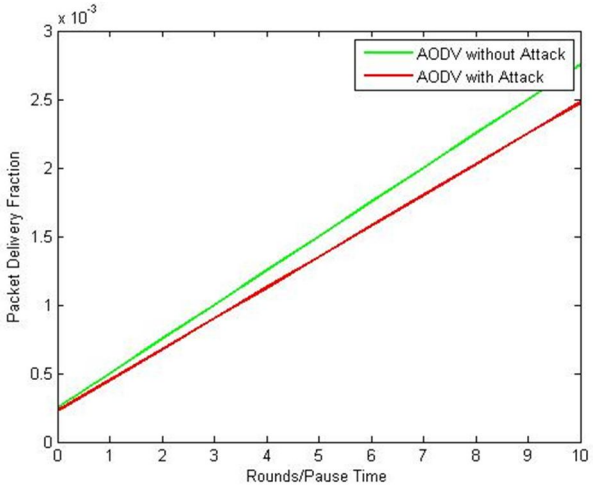


Fig5.e: Packet Delivery Fraction

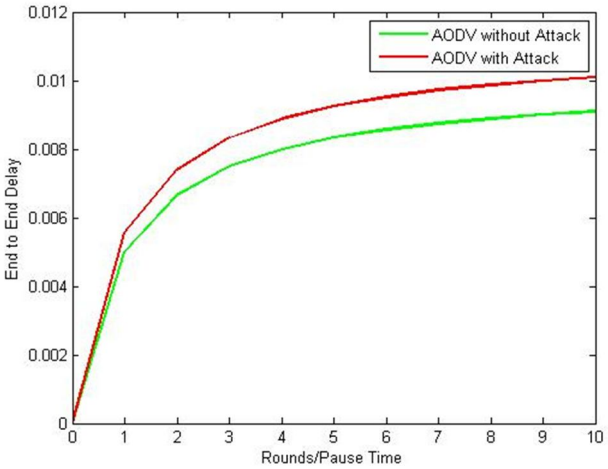


Fig5.f: End to end Delay in presence of Attacks

ENCRYPTION SCHMES with CHAOS THEORY:

MESSAGE for ENCRYPTION:

50 67 246 168 136 90 48 141 49 49 152 162 224 55 7 52

ADVANCE ENCRYPTION STANDARD (AES):

S-BOX:

99 124 119 123 242 107 111 197 48 1 103 43 254 215 171 118
202 130 201 125 250 89 71 240 173 212 162 175 156 164 114 192
183 253 147 38 54 63 247 204 52 165 229 241 113 216 49 21
4 199 35 195 24 150 5 154 7 18 128 226 235 39 178 117
9 131 44 26 27 110 90 160 82 59 214 179 41 227 47 132
83 209 0 237 32 252 177 91 106 203 190 57 74 76 88 207
208 239 170 251 67 77 51 133 69 249 2 127 80 60 159 168
81 163 64 143 146 157 56 245 188 182 218 33 16 255 243 210
205 12 19 236 95 151 68 23 196 167 126 61 100 93 25 115
96 129 79 220 34 42 144 136 70 238 184 20 222 94 11 219
224 50 58 10 73 6 36 92 194 211 172 98 145 149 228 121
231 200 55 109 141 213 78 169 108 86 244 234 101 122 174 8
186 120 37 46 28 166 180 198 232 221 116 31 75 189 139 138
112 62 181 102 72 3 246 14 97 53 87 185 134 193 29 158
225 248 152 17 105 217 142 148 155 30 135 233 206 85 40 223
140 161 137 13 191 230 66 104 65 153 45 15 176 84 187 22

ENCRYPTED MESSAGE with S-BOX:
137 237 94 106 5 202 118 51 129 53 8 95 226 28 64 189

DECRYPTED MESSAGE with S-BOX:
50 67 246 168 136 90 48 141 49 49 152 162 224 55 7 52

ADVANCE ENCRYPTION STANDARD(AES) with CHAOS THEORY:

CHAOS S-BOX :

42 101 205 85 180 138 238 19 59 132 246 9 38 93 190 110
220 48 115 230 33 83 177 145 221 47 114 229 34 84 179 139
235 26 73 158 193 105 210 70 154 199 97 198 98 201 92 189
113 228 35 86 181 136 240 15 54 126 255 0 16 56 129 251
4 23 65 143 223 44 109 218 52 120 237 22 64 142 224 43
106 211 69 153 200 94 191 108 216 55 127 254 1 17 57 130
250 5 25 72 156 195 103 207 75 163 174 149 213 66 144 222
46 112 227 36 87 182 133 245 10 41 100 203 89 186 123 247
8 37 90 187 122 244 11 45 111 225 40 96 197 99 202 91
188 118 233 28 77 167 164 173 150 212 68 152 204 88 183 128
253 2 20 61 135 242 13 50 117 232 29 78 169 161 178 141
226 39 95 192 107 214 62 137 239 18 58 131 248 7 32 81
172 151 208 74 160 184 125 252 3 21 63 140 234 27 76 166
165 168 162 176 147 217 53 121 241 14 51 119 236 24 67 146
219 49 116 231 30 79 170 159 185 124 249 6 31 80 171 157
194 104 209 71 155 196 102 206 82 175 148 215 60 134 243 12

ENCRYPTED MESSAGE with CHAOS S-BOX:

193 7 1 18 105 124 147 244 179 219 203 114 249 32 120 225

DECRYPTED MESSAGE with CHAOS S-BOX:
50 67 246 168 136 90 48 141 49 49 152 162 224 55 7 52

IX. CONCLUSION

The paper proposes a novel method for autonomic computing in WSN by three features Self-optimization, self-protection and transactional security. The proposed approach for self-optimization uses PSO based cluster head selection for efficient network lifetime. Results show that proposed system outperforms the existing cluster head selection methods in terms of network throughput, end to end delivery ratio and network lifetime. Watch mechanism based approach is proposed for self-protection by monitoring malicious nodes and black hole detection. It is depicted in results that how the existence of malicious nodes affects the system performance. Furthermore Chaos based AES cryptography has been proposed to provide transactional security to the network. Simulation has been carried out on MATLAB. The overall impact of aforementioned schemes is to provide Transactional security and to enhance network lifetime by applying autonomic characteristics to WSN.

X. REFERENCES

[1] Kephart, J. O. and Chess, D. M. (2003). The vision of autonomic computing. *IEEE.*

[2] Markus c. Huebscher, julie a. Mccann "A survey of Autonomic Computing -degrees, models and applications" .

[3] Radu Calinescu, **"**General-Purpose Autonomic Computing."

[4] G.M.P. O'Hare, M.J. O'Grady, D. Marsh, A. G. Ruzzelli and R. Tynan, "Autonomic Wireless Sensor Networks: Intelligent Ubiquitous Sensing".

[5] Max do Val Machado, Olga Goussevskaia, Raquel A. F. Mini, Cristiano G. Rezende, Antonio A. F. Loureiro, Geraldo Robson Mateus, and José Marcos S, " Data Dissemination in Autonomic Wireless Sensor Networks" ieee journal on selected areas in communications, vol. 23, no. 12, december 2005.

[6] Braga, T. Silva, F. ; Nogueira, J.M. ; Loureiro ,"A Tiny and Light-Weight Autonomic Element for Wireless Sensor Networks" ICAC '07.

[7] Tynan, R. ;O'Hare, G.M.P. Ruzzelli, "Autonomic Wireless Sensor Network Topology Control Networking, Sensing and Control", 2007 IEEE International Conference April 2007

[8] Di Pietro, R. Mancini, L.V. Soriente, C. Spognardi, A. "Data Security in Unattended Wireless Sensor Networks Computers", IEEE Transactions on Vol:58 , Issue: 11 Nov. 2009.

[9] Igor M. B. Spadoni, Regina B. Araujo, Cesar Marcondes, "Improving QoS in Wireless Sensor Networks through Adaptable Mobile Agents" Ieee Infocom workshop 2009.

[10] K. Saleem, N. Fisal, S. Hafizah, S. Kamilah, and R. A. Rashid, "A Self-Optimized Multipath Routing Protocol for Wireless Sensor Networks". International Journal of Recent Trends in Engineering, Vol 2, No. 1, November 2009.

[11] Georgios Smaragdakis Ibrahim Matta Azer Bestavros "SEP: A Stable Election Protocol for clustered heterogeneous wireless sensor networks", In: Proc. of the Int'l Workshop on SANPA 2004.

[12] Yu Wang Xiang-Yang Li Qian Zhang ,"Efficient Self Protection Algorithms for Static Wireless Sensor Networks".

[13] J. O. Kephart and D. M. Chess, "The vision of autonomic computing," IEEE Computer, vol. 36-1, pp. 41-50, January 2003.

[14] D. Marsh, R. Tynan, D. O'Kane and G. M. P. O'Hare, "Autonomic Wireless Sensor Networks," Engineering Applications of Artificial Intelligence, vol 17-7, pp. 741-748, October 2004.

[15] M. Wooldridge and N. Jennings, "Intelligent Agents: Theory and Practice", Knowledge Engineering Review, vol. 10-2, pp. 115-152, 1995.

[16] A. Ruzzelli, G. M. P. O'Hare, M. J. O'Grady, R. Tynan, "Adaptive scheduling in wireless sensor networks," 2nd IFIP International Workshop on Autonomic Communication (WAC 2005), Vouliagmeni, Athens, Greece, October 3rd-5th, 2005.

[17] H. Qi, P. T. Kuruganti, Y. Xu, "The development of localized algorithms in wireless sensor networks," Sensors, vol. 2, pp 286- 293, July 2002.

