International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 4, Issue 6 (October 2012), PP. 45-53

Development of Efficient Memory management, Intrusion Detection & Authentication methods for designing adaptive reprogramming in Wireless Sensor Networks

Veena Gulhane[1], Dr.L.G.Malik[2]
[1]*Assistant Prof., Computer Science & Engineering. Department. , G.H. Raisoni College of Engineering, RTM University, Nagpur, M.S., India*
[2]*Professor. Computer Science & Engineering Department. , G.H. Raisoni College of Engineering, RTM University, Nagpur, M.S., India.*

Abstract: *Building adaptive WSN applications through reprogramming is a fantastic area. Recent research in wireless sensor networks (WSNs) has highlighted the importance of supporting the capability for remote reprogramming of sensor nodes via wireless network. Ease of programming has long been recognized as a major hurdle to the adoption of WSN technology. There are lots of key issue & open problems that need further investigation to make reprogramming highly usable and efficient. This paper focus on the three different methods designed by us & its analysis which considers main key issues of WSN like Memory management, Intrusion Detection & Authentication & will be helpful for designing adaptive reprogramming in Wireless Sensor Networks.*
Keywords: *Wireless Sensor Networks (WSN), Network Reprogramming, Buffer management, Compression of data, Data security, Intrusion Detection, Authentication.*

I. INTRODUCTION

There are many reasons why reprogramability is in a significant need for deploying WSNs. It is a crucial issue for the acceptance of WSNs in most major fields. Reprogrammability, also known as reconfiguration or retasking, refers to as the capacity of being able to deploy applications dynamically to WSNs without the need of manual intervention. Typical wireless sensor network (WSN) consists of a large number of small-sized battery-powered sensor nodes that integrate sensing, computing, and communication capabilities. In most applications sensor networks are deployed once in the designated area like geophysical /structural/habitat monitoring, security surveillance, disaster area or battlefield information collection, and pervasive computing, will be expected to operate the sensor node for extended periods of time, without any human intervention. Wireless sensor networks are expected to be deployed for long periods of time. Software already installed in sensor nodes may need to be updated with new functionalities or features; nodes are likely to need remotely patch or upgrade software during their lifetime, both for bug fixes and in order to support new requirements.

Dynamic reprogramming of sensor applications and sensor operating systems is emerging as a critical function required in wireless sensor networks. This ability to remotely patch or upgrade software in deployed sensor nodes via the wireless network is complicated by the increasing trend towards heterogeneity in WSN hardware platforms, sensor operating systems and role-based differentiation, e.g. between aggregators and leaf sensor nodes.

Several platform dependent programming solutions have been hitherto developed. A well-established characterization of the available approaches are, however, largely missing. As a result, researchers are unable to orient themselves in this diverse, and developers struggle in identifying the solutions most appropriate to their application requirements. [6]

Most of current network reprogramming protocols focus on propagating the same code image to a network of homogeneous sensor nodes. Naive approaches to adapt such protocols for heterogeneity are largely inefficient. The OAPs developed do not support security. Unfortunately, security mechanisms like public key cryptography and other mechanisms were not compatible with the resource constrained devices like sensor nodes until recently. As a result, security remained a neglected aspect of OAP for some time. Development of strong and secure methods of security and authentication for OAP is needed. Also need to consider is security and robustness issues, including intrusion detection, integrity, privacy, authentication, reliability, intermittent disconnections, link failures, and so forth. The challenges mostly arise from the WSN's limitations on resources and capacities.

The remainder of this paper is organized as follows.

- Various key issues for designing and implementing adaptive reprogramming in Section II.

- Efficient Memory management, Intrusion Detection & Authentication methods are discussed in Section III, IV, & V respectively.
- Section VI gives the performance & Analysis of the methods discussed in previous three sections.
- Section VII concludes the paper.

II. Various Key Issues for Designing and Implementing Adaptive Reprogramming & Constrained Capabilities of Sensor Nodes.

A. Key Issues

1) Handling efficient exchange of code image in multihop reprogramming,
2) Minimizing packet flooding by efficient management of different versions of image code,
3) Initializing route repair and route discovery,
4) Reducing size of script code,
5) Providing secured authentication and dissemination in hybrid wireless (Heterogeneous) optimized multihop code generation,
6) Updating critical code and application code for adaptive dynamic reprogramming,
7) Reducing control overhead while advertisement,
8) To provide efficient memory management for code image creation and execution.

B. *Constrained Capabilities*

There is no. of constrained capabilities & limitations of of sensor node that complicate the routing protocols, security design and deployment in sensor networks.

1) Hostile Environment
2) Random topology
3) Power restrictions
4) Limited Computational power
5) Error-prone wireless medium.
6) Fault tolerance and adaptability.

It is important to understand the constrained capabilities of sensor nodes performance against sensor nodes' limitations.

Each host sets a maximum buffer size that it is willing to allocate for message distribution. The buffer size limits the amount of memory and network resources consumed through routing.

WSNs suffer from a wide range of security attacks due to their limited processing and energy capabilities. Their use in numerous mission critical applications, however, requires that fast recovery from such attacks be achieved.

III. Efficient Memory Management By Developing Space Based Buffer Management Scheme Using Compression. [4]

Buffer management policy is very important for wireless sensor network. The capacity of the available buffer of each node in network is limited leads to congestion in the network .Until now many buffer management policies for WSN are adopted which are based on queuing policies. The proposed compression technique helps to reduce the burden on the buffer and increases the throughput of the network. But when there are finite buffers in the network, problem may arise when these buffers get full. The proposed compression technique is implemented on hardware and operates real-time to capture data. For the implementation of proposed compression technique we have used a hardware called AVR kit AT mega 32.There are two kits which are act as two nodes in the network. These two nodes are sending data packets in form of bytes to each other. For the data compression we are used Run Length encoding algorithm which show that the proposed technique gives better compression result compared to prior work discussed in [1].

A. Objectives of the Study:

The objective of this study is to develop an efficient space based buffer management using compression.

1) *Latency:* the average duration between a message's generation and the arrival time at the last destination.

2) *Compression:* makes space in buffer for incoming node when the buffer is overflow. For maximization of the message deliveries and minimization of the average delay, two utility functions are proposed on the basis of message properties, the number of replicas and the remaining time-to-live.

B. Technique used in Buffer Compression:

First of all Huffman coding will take all the input data from the network. Then after execution of this algorithm, output obtained in bit stream format. This output is given as input to Run Length Encoding to get the compressed data of buffer. With the help of this algorithm, we try to minimize buffer load by compression. We focus on buffer overflow, if buffer gets overflow then by using this two algorithms we compress the data in the buffer.

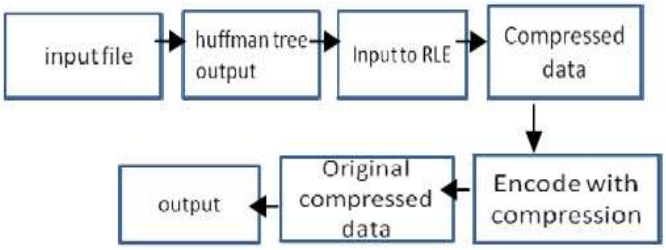

Fig: 1 - Block dig of proposed system.

Fig. 1 Shows the proposed system for buffer compression. Once we get input from nodes in the wireless network, then we apply Huffman coding for compression of data this will give us about 50% compressed data, but for more efficient compressed data, we then apply RLE to the input which is coming from Huffman coding. So, this will give us about 70% compression in buffer.

Fig .2. Shows how this two algorithms work in the combination. First of all code loads the input buffer and calls compression algorithm. This will compresses data to the output buffer, and then again by applying other processing it will compress data and end with compression. By applying the reverse process for decoding we will get the original output at end of the algorithm.

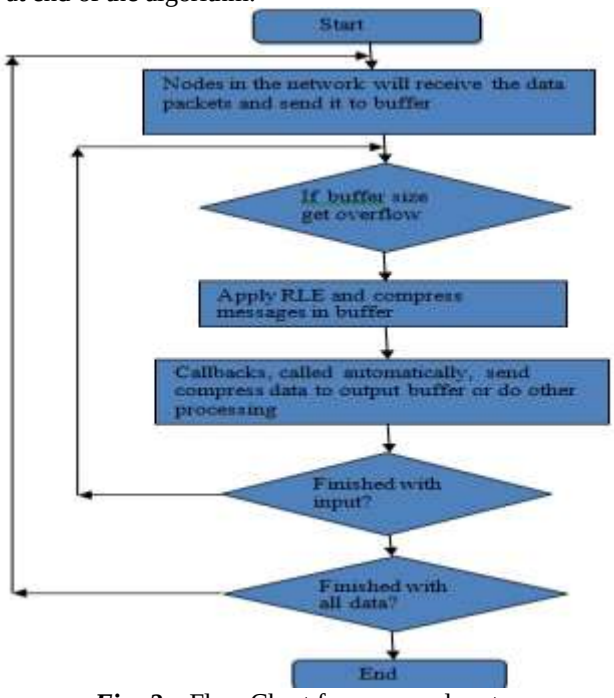

Fig: 2 **–** Flow Chart for proposed system.

C. Impact Of Buffer Size On Network [2]

Each host sets a maximum buffer size that it is willing to allocate for message distribution. The buffer size limits the amount of memory and network resources consumed through routing. Of course, there is an inherent trade-off between aggregate resource consumption and message delivery rate/latency. To ensure eventual delivery of all messages, the buffer size on at least a subset of nodes must be roughly equal to the expected number of messages in transit at any given time. i.e., Routing works with the assumption of availability of infinite buffers. But this is not the case in reality. In order to cope with long disconnections, messages must be buffered for long period of time.

This means that intermediate routers require enough buffer space to store all the messages that are waiting for future communication opportunities. To limit total resource consumption is to bind the amount of buffer space available for routing. However, it is typically possible to achieve robust delivery rates with substantially less buffer space. In general, the different nodes will have different buffer capacities.

D. Performance Comparison:

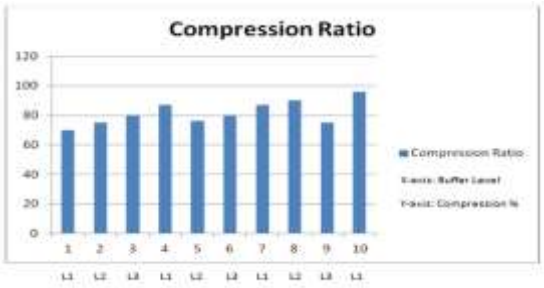

Fig 3: Comparison in form of compression ratio

Figure 3 shows graphical representation for various outputs in form of compression ratio. 1, 2, 3 shows compression ratio for level L1, L2, L3 again 4, 5, 6 shows compression ratio for level L1, L2, L3 and similarly 7, 8, 9 for level L1, L2, L3 are respectively on X-axis. And Y-axis shows compression percentage for each level respectively.

D. Description :

With the help of this algorithm, we try to minimize buffer load by compression. We focus on buffer management in nodes; if buffer gets full then by using RLE we compress the data in the buffer. EEPROM (Electronically Erasable Programmable Read Only Memory) is used as buffer at these two nodes. EEPROM is inbuilt memory in AVR kit AT mega 32 .In the 1st module we showed that RLE is better to use than Huffman Coding. And we showed C code for Run Length Encoding. There are two AVR kits AT mega 32 which are act as two nodes in the network. These two nodes are sending and receiving data with the help of transceiver. There is a buffer of size 512 bytes. If this buffer gets full then we apply Run Length Encoding so that it will compress the recursive bits and make space for new incoming node in the network. By dumping C code into the AVR kit we can compress the buffer size so that new incoming data will get the space in buffer. Once we get input from nodes in the wireless network, and if the buffer size gets full then we apply RLE to the input So that it will give us about 80% to 90% compression in buffer. Also we showed graphical representation for compression ratio by taking various inputs at level L1, L2, L3.

IV. An Intrusion Detection Using Hybrid Technique In Cluster Based Wireless Sensor Network[5]

In many important military and commercial applications, it is critical to protect a sensor network from malicious attacks, which presents a demand for providing security mechanisms in the network. The WSN is vulnerable to security threats and susceptible to physical capture. Thus, it is necessary to use effective mechanisms to protect the network. Intrusion detection system is one of the major and efficient defensive methods against attacks on wireless sensor network. Sensor networks have different characteristics and hence security solutions have to be designed with limited usage of computation and resources. In this paper, the architecture of hybrid intrusion detection system (HIDS) has been proposed for wireless sensor networks. In order to get hybrid scheme, the combined version of Cluster-based and Rule-base intrusion detection techniques is used and eventually evaluated the performance of this scheme by simulating the network. The simulation result shows that the scheme performs intrusion detection using hybrid technique and detection graph shows ratings like attack rating, data rating and detection net rating with the attack name and performs better in terms of energy efficiency and detection rate.

A. System Architecture and Network Model

The proposed HIDS consists of an intrusion detection module and decision making module. Intrusion detection module filters a large number of packet records using the rule base technique. Decision making module is used to take an administrative action on the false node with the help of base station.

System Architecture and Network Structure

Here, the new Hybrid Intrusion Detection Model (HIDS) is proposed for Cluster Based Wireless Sensor Network (CWSN). This consists of two modules as shown in Figure 4. First, the Intrusion Detection

Engine is used to filter the incoming packets and classify is as normal or abnormal. The packets identified as an abnormal are passed to the decision making module. The decision-making module is used to determine whether the intrusion occurs and the type of intrusion or attacks behavior. Finally, the decision making module returns this information to the base station to follow-up treatment on intruder node.

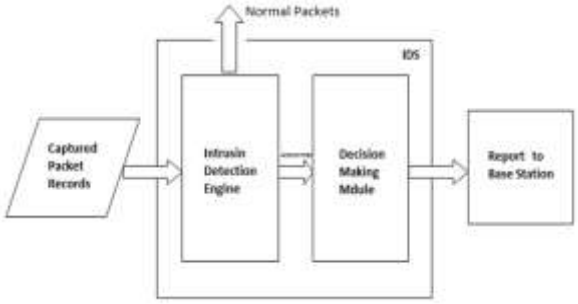

Figure 4 . Proposed System Architecture

In this proposed model, we used a hierarchical topology that divide the sensor network into clusters, each one having a cluster head (CH) .Here the sensors nodes are fixed and assuming that the cluster heads having the more energy than the other sensor nodes. The objective of this architecture is to save the energy that allows the network life time prolongation and reduce the amount of information in the network.

B. *IDS Techniques Used*

In the proposed Hybrid Approach [8] [9], the two techniques i.e. Cluster-Based and Rule-Based techniques are merged to form Hybrid Intrusion Detection technique. Hybrid detection used to gain the advantages of both Cluster-Based approach and Rule-Based approach. This combination provides simplicity, easy to operate, low consumption of energy and provide high safety. The Hybrid Intrusion Detection System (HIDS) achieves the goals of high detection rate and low false positive rate.

1) *Cluster-Based:* Clustering is known as hierarchical of WSN [10]. To divide the network nodes into head cluster and members of nodes is the basic idea. Cluster head is the centre of a cluster. Through cluster head's information fusion and forwarding to the member node of cluster, other members of nodes transmit to the base station.

Function of Base Station:
- All nodes are able to send data to BS via Cluster Head.
- Base station has all the information regarding each Cluster (number and MAC address).
- The removal or addition of any node in a Cluster is monitored by the Base Station.
- Poll status of each node is received with MAC address.
- Base station runs task of MAC address tracking, MAC address history and management of database.
- The Base Station has the capability to seize the operation of any node in the network.

Function of Cluster Head:
- Cluster Heads keep track of each node and sends periodic status information to the Base Station.
- Cluster heads receives data from its nodes and sends necessary information.
- Cluster Heads (CHs) transmits data to Base Station after performing data reception and compression.

2) *Rule-based. :* Rule-based intrusion detection [11] is the collection and classification of data, the data is placed in a queue, using the FIFO principle. In our model while monitoring the network this rules are selected appropriately and applied to the monitored data. If the rules defining an anomalous condition are satisfied, an intrusion is declared. The algorithm has three phases for detecting intrusions. In the first phase monitor nodes monitors the data. In the second phase the detection rules, are applied, in increasing order of complexity, to the collected information to flag failure. The third phase is the intrusion detection phase, where the number of failure flagged is compared to the expected number of the occasional failures in the network. Occasional failures include data alteration, message loss, and message collision. An intrusion alarm is raised if the number of failures flagged exceeds the expected number of occasional failures. The rule base methods are fast, simple and require less data.

Rules and Definitions:

Development of this IDS to a target cluster-based WSN are divided into three following important steps:

- Pre-select, from the available set of rules, those that can be used to monitor the features defined by the designer;
- Compare the information required by the pre-selected rules with the information available at the target network to select rules definitively; and
- Set the parameters of the selected rules with the values of the design definitions.

Definitions of the rules used are presented in the following:

- *Integrity Rule:* to avoid data fusion or aggregation by other sensor nodes, the message payload must be the same along the path from its origin to a destination. Attacks where the intruder modifies the contents of a received message can be detected by this rule.
- *Jamming Rule:* the number of collisions associated with a message must be lower than the expected number in the network. The jamming attack, where a node introduces noise into the network to disturb the communication channel, can be detected by this rule.
- *Interval Rule:* if the time interval between the receptions of two consecutive messages is longer or shorter than the allowed time limits, a failure is raised. Two attacks that will probably be detected by this rule are the negligence attack and the exhaustion attack. In the negligence attack, the intruder does not send data messages generated by a tampered node. While in the exhaustion attack, the intruder increments the message-sending rate in order to increase the energy consumption of other nodes in the cluster.
- *Repetition Rule:* the same message can be retransmitted by a node only a limited number of times. This rule can detect an attack where the intruder sends the same message several times, thus promoting a denial of service attack.
- *Radio Transmission Range:* all messages listened to by the monitor node must be originated from one of the nodes within its cluster. Attacks like wormhole and hello flood, where the intruder sends messages to a far located node using a more powerful radio, can be detected by this rule.
- *Retransmission Rule:* the monitor listens to a message, pertaining to one of its neighbours as its next hop, and expects that this node will forward the received message, which does not happen. Two types of attacks that can be detected by this rule are the blackhole and the selective forwarding attack. In both of them, the intruder suppresses some or all messages that were supposed to be retransmitted, preventing them from reaching their final destination in the network.
- *Delay Rule:* the retransmission of a message by a monitor's neighbor must occur before a defined timeout. Otherwise, an attack will be detected.

C. *Algorithm:*

Algorithm 1: Rules application procedure of IDS

```
1: for all messages in data structure array do
2: for all rules specific to the message in descending order by
weight do
3: apply rule to the message;
4: if (message == fail) then
5: increment failure counter for the node based on weight;
[failure counter = failure counter + weight]
6: discard message;
7: break;
8: end if
9: end for
10: discard message;
11: end for
```

Algorithm 1 shows the procedure of rules application on messages in the network. The algorithm applies rules on all the messages. If message fails according to the rule, then the failure counter will incremented and discards all the messages.

D. *Network Simulation Results*

In this proposed architecture, the wireless sensor network is divided into the small clusters. The hierarchical clustering is used to divide the sensor nodes. After the clustering process finished, the cluster head have been selected dynamically according to the current status of the nodes and formed the Cluster based WSN .Generally, the node having highest energy left elected as a cluster head. Simulation runs with the following simulation parameters:

1	Routing Protocol	AODV
2	Mac Layer Protocol	802.11
3	Total No. Of Nodes	50
4	Traffic type	CBR
5	Simulation Topology	1024cm x 768cm
6	Simulation Time	100 sec
7	Packet size	512 Kbytes

Table 1: . Simulation parameters

Nodes are deployed randomly over an area of 1024 cm X 768 cm. The node closest to the centre of the deployment area is selected as sink or base station (BS), which is resources not limited, secure and safety for any advisory attackers and acts as an administrator for taking appropriate action on the intruder nodes. The network performance is observed for the simulation time 100 sec. The standard packet size is used i.e. 512 Kbytes.

The detection of the attacks is shown in Figure 5 with their ratings and names. The wormhole, blackhole and syncflood attacks have been detected.

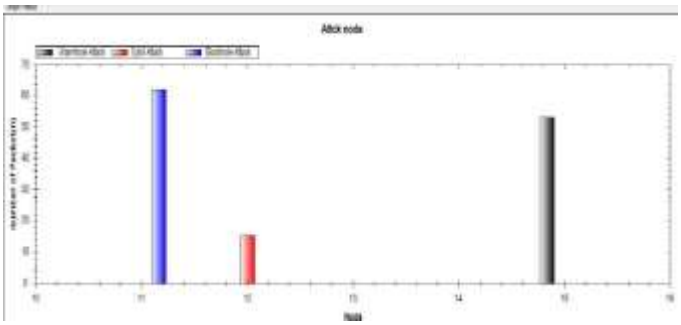

Figure 5 . Intrusion detection Graph

V. User Authentication Using Colors And Data Security Using Armstrong Numbers For Wireless Sensor Networks [4]

In real world, data security plays an important role where confidentiality, authentication, integrity, non repudiation are given importance. This paper, proposes a User Authentication (UA) scheme for Wireless Sensor Networks (WSNs), which employs RGB color cube algorithm and Armstrong number for data security. The simulation results shows that proposed scheme is not only secure but also increase speed of communication than the existing ATTUA scheme [12].

A. System Model

In the proposed scheme WSN consists of,

- Base station with high processing capability.
- Sensor nodes having low processing capability with less power.
- Users with no power constraints compared to sensor nodes.

Users interact with the WSN for data query and retrieval. After processing sensed information; the sensor node either sends the data upon event detection or stores it to serve for the next query. Between user and Base station RGB based authentication algorithm is used. And also Armstrong number based security algorithm is used in which 128 bit key is generated using Armstrong number and which is used in AES algorithm for data encryption and decryption.

B. RGB Based Authentication

The proposed scheme includes two phases: Registration & Authentication.

1) *User registration:* user module selects RGB color value for the user and then finds the position of this RGB in the cube and send request with its ID and POS to the base station for registration in WSN. Base station generate a random number Which is termed as seed .Also the base station module scales the seed value with the Armstrong number and multiply it with the POS it received from the user. It performs MD5 on this product and

generate 128 bit key which is used for data security in AES algorithm. Base station send the key and seed to user and store the values in its database. User upon receiving store the POS,SEED,KEY in its database.

2) *User Authentication on Login:* In this phase user find out the new position of RGB using RGB color cube and PRNG in which the user module generate next random number using PRNG in which it uses the seed received from the base Station in the registration phase and then offsets its previous RGB POS to NEW_POS with this new SEED_NEW and login with its ID and H[POS_NEW] to the base station. Upon Login request base station also generate the SEED_NEW using PRNG and find out the POS_NEW1 in the RGB cube. If the POS_NEW matches POS_NEW1 the user is authentic.

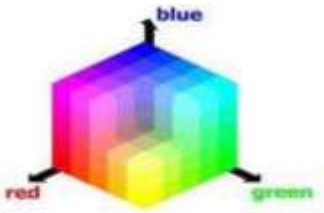

Figure.6: RGB Color Cube

The three primary colors of the additive color model are red, green, and blue. This RGB color cube displays smooth transitions between these colors. It has 8 bits per components.256 * 256 * 256 numbers of possible colors. Each color represented by a number in the cube (POS):

POS = r + (g*256) + (b*256*256)

C. Pseudo RNG

Uses 'seed' state. A PRNG can be started from an arbitrary starting state using a seed state. It will always produce the same sequence thereafter when initialized with that state.

The period of a PRNG is defined as the maximum over all starting states of the length of the repetition-free prefix of the sequence. The period is bounded by the size of the state, measured in bits. However, since the length of the period potentially doubles with each bit of 'state' added, it is easy to build PRNGs with periods long enough for many practical applications uniformly distributed random numbers. If 2 parties use same seed on the same PRNG, it will deterministically give the same next number.

Xn+1 = F (Xn)

D. Data Security

Upon successful authentication base station encrypts the requested data with the key generated using Armstrong number in AES algorithm and send data to the user then user decrypt data using AES algorithm with the key generated using Armstrong number.

E. *Performance Comparison*

	RGB based authentication	ATTUA
Average time required for registration	0.000173 seconds	0.166563628 seconds
Average bytes required for registration	67 Bytes	68 Bytes [256 bit public/private key]
Average time required for login	0.000152 seconds	0.002171226 seconds
Average bytes required for login	40 Bytes	104 Bytes

Table 2.Performance Comparison

- *Simulation Parameters: The* RGB based user authentication scheme is implemented On NS2.34 with 5 sensor nodes randomly distributed over 670x670m2. Number of users 10 and one base station node. Simulation time1099.000703seconds .

VI. PERFORMANCE & ANALYSIS

As per discussion in section III, we investigate the buffer management problem in mobile Network. First of all we showed the performance of RLE on various strings. And result show that RLE algorithm is better when it applies on large number of string. The proposed scheme for buffer compression uses RLE algorithm.

When the buffer of a node is full, this buffer compression technique gives the result about 70% to 80% compression as compared to existing techniques of buffer management. This will reduce the problem of buffer overflow in the network. Results indicate that our approach yields better compression at each node in mobile networks.

As per discussion in section IV, we proposed hybrid model of intrusion detection for WSN. This detection framework is evaluated and demonstrated and it is effective, even when the density of the network is high and there is a high probability of collisions in WSNs. In addition, the detection modules involve less energy consumption than techniques proposed in previous works because here cluster based technique is used. The simulation setup creates the behavior of attacks into the network and detected wormhole, blackhole and sybil attacks.

As per discussion in section V, we proposed a user authentication scheme for wireless sensor network named RGB based authentication scheme. This scheme provides sufficient security for sensor nodes having less processing capability. Simulation results have shown that the RGB based authentication scheme requires less time for registration and login, also bytes consumed by the proposed scheme is less than the existing schemes.

VII. CONCLUSION

Reprogramming sensor nodes is more economical and practical than deploying new sensor nodes. In this paper, we have discussed the three different methods designed by us in our existing work. From the analysis of these schemes we can conclude that these methods will be helpful for designing adaptive reprogramming in Wireless Sensor Networks. Our work is in progress to design & implement a real time reprogramming architecture for Wireless Sensor Networks in which the techniques of the methods discussed in this paper will play an important role to design more robust solution for WSNs.

References

[1] Ms. Amruta A. Deshmukh, Mrs. Veena Gulhane, "*Space Based Buffer Management in Mobile Networks by Using Compression"* International Conference on Computers & Communication **S**agar Institute of Science & Technology, Bhopal **J**anuary 27- 28, 2012.

[2] Shakera Shaikh & Veena Gulhane, "*User Authentication Techniques for Wireless Sensor Networks: A Survey*", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248-9738 Volume-1, Issue-4, 2012.

[3] Ms. Amruta A. Deshmukh[1], Mrs.Veena Gulhane[2], "*Use of Compression Technique to Improve Efficiency of Buffer in Mobile Network",* International Journal of Advanced Research in Computer Science and Electronics Engineering Volume 1, Issue 3, May 2012, ISSN: 2277 – 9043.

[4] Shakera Shaikh & Veena Gulhane, "*User Authentication using Colors and data security using Armstrong numbers for Wireless Sensor Network",* International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-1, Issue-1, and June 2012.

[5] Mr. Sumedh G. Dhengre, Mrs. Veena Gulhane, "*An Intrusion Detection Using Hybrid technique in Cluster based Wireless Sensor Network*", International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 3 May – 2012, ISSN: 2278-0181.

[6] Mr. Sumedh G. Dhengre, Mrs. Veena Gulhane, "*Analysis of Intrusion Detection System for Wireless Sensor Network*", 2012 International Conference on Electronics Computer Technology (ICECT 2012).

[7] B. Li, L.M. Batten, Senior Member, IEEE and R. Doss, Member, IEEE, "*Lightweight Authentication for Recovery in Wireless Sensor Networks",* 2009 Fifth International Conference on Mobile Ad-hoc and Sensor Networks.

[8] K. Q. Yan, S. C. Wang, S. S. Wang and C. W. Liu, "*Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network*", Chayang University of Technology, Taiwan, IEEE 2010, pp. 114-118 .

[9] K. Q. Yan, S. C. Wang, S. S. Wang and C. W. Liu, "*Hybrid Intrusion Detection of Cluster-based Wireless Sensor Network*", Proceedings of International Multi Conference of Engineers and Computer Scientists , Hong Kong, Vol. 1, 2009.

[10] S. Doumit and D. P. Agrawal, "*Self-organized Critically & stochastic learning based intrusion detection system for wireless sensor network",*MILCOM2003-IEEE/ACM transactions on Networking, Vol. 11(1), 2003, pp 2-16.

[11]. S. Northcutt and J. Novak, "*Network Intrusion Detection: An Analyst's Handbook*," New Riders Publishing, Thou-sand Oaks, 2002.

[12] Ismail Butun and Ravi Sankar, 2011. "*Advanced Two Tier User Authentication Scheme for Heterogeneous Wireless Sensor Networks".*2nd IEEE CCNC Research Student Workshop.

[13] X.H. Le, S. Lee, and Y.K. Lee. "*Two-Tier User Authentication Scheme for Heterogeneous Sensor Networks." the 5th IEEE International Conference on Distributed Computing in Sensor Systems,* (DCOSS '09), Marina Del Rey, California, USA, June 8-10, 2009.

[14] Qiang Wang, Yaoyao Zhu, and Liang Cheng, Lehigh University, "*Reprogramming Wireless Sensor Networks: Challenges and Approaches*", IEEE Network • May/June 2006.

[15] Jun-Zhao Sun ,Academy of Finland , "*A CFSM-based Reprogramming Scheme for Flexible Wireless Sensor Networks",* International Conference on Frontier of Computer Science and Technology,2009.

[16] B. Li, L.M. Batten, "*Lightweight Authentication for Recovery in Wireless Sensor Networks",* 2009 Fifth International Conference on Mobile Ad- hoc and Sensor Networks.

[17] Huang Ruo-Hong , "*Two Energy-Efficient and Timesaving Improvement Mechanisms for Network Reprogramming in Wireless Sensor Network*", 2nd international Conference on Education Technology and Computer (ICETC), 201 0.