Distributive Reprogramming of Wireless Sensor Nodes with Secure Data Transmission

B. Navin, S. Benila

Abstract*— Wireless sensor networks have found their applications in numerous industrial fields. This is because they assist humans by ceaseless monitoring of impossible areas by sending timely updates to the base station. Once these sensors are set up, it is highly impossible for humans to manually reprogram such devices and hence a reprogramming protocol is a necessity here. Such a reprogramming process needs to be done in an energy efficient way. This paper we propose Distributive Reprogramming of sensor nodes with secure Data Transmission where the nodes are categorized into good and bad nodes during the forwarding process of the reprogramming code. Also a random key generation and exchange is proposed and used between the nodes in this work to further improve security. Also the allocation of the Users in SDRP is a significant task as the failure of the User Node might cause the failure of the entire group of nodes under that particular User. Considering the energy of each wireless sensor node the allocation of the users can be done to enhance the overall energy efficiency of the SDRP without altering the multi-authorization of the network. It is an enhancement over Secure and Distributive reprogramming protocol and has been proved through network simulator simulations to show greater quality of service on Energy, Packet loss, Delay and throughput than the existing scheme.

***Index Terms*—Diffie-Hellman key exchange, reprogramming, security, sensor networks, user privilege.**

I. INTRODUCTION

Wireless sensor networks (WSNs) have gained the entire world's attention for its use in different applications, in the recent years. Each Sensor node is placed across a large area of interest to monitor and sense information in order to transmit the data to the user. The nodes are typically equipped with radio transceivers, micro-controllers, and batteries. Sensor nodes that are small in size, low power devices, could be deployed in large numbers and in a spatial distribution. They can be used in applications such as military target tracking and surveillance, biomedical health monitoring, natural disaster relief, and industrial automation. Wireless reprogramming is the process of propagating a new code image or significant commands to sensor nodes through wireless links after a wireless sensor network (WSN) is deployed. It is very essential in order to remove fatal bugs during the WSN operations and also to either upgrade or improve the functionalities. Generally, a WSN is generally deployed in hostile environments such as the battlefield or a power plant, a place where an attacker may exploit the reprogramming mechanism to launch various fatal problems.

Manuscript received on May 18, 2014.

B. Navin, Computer Science and Engineering/ Valliammai Engineering College, Chennai, Tamil Nadu.

S. Benila, Computer Science and Engineering/ Valliammai Engineering College, Chennai, TamilNadu.

Thus, secure programming is and will persist to be a major concern. Even though many schemes propose secure reprogramming, all of them are based on the centralized approach which assumes the existence of a base station where the base station alone has the authority to reprogram sensor nodes. In Secure and Distributed Reprogramming Protocol (SDRP), the protocol provides security for data packets. However it cannot provide enhanced quality of service. In some applications quality of service is a main necessity. So they cannot keep the data packets with secrecy. In this paper, we propose the Packet Dropper Free Secure and Distributed Reprogramming Protocol (PDF – SDRP). It provides more efficient secure for data packets. We use Node categorization algorithm, so it can keep the packet droppers away and it can provide security for each and every packet without losing the features of SDRP. So anyone can't slash the information. Figure 1, shows an example scenario where many wireless sensor nodes sense information and transmit to the base station.

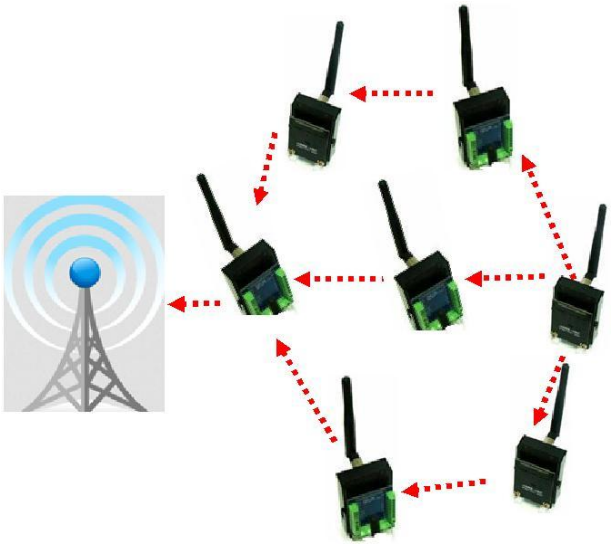

Figure 1. Example of a Wireless Sensor Network

II. RELATED WORK

There are many research work efforts that reprogramming problems. The technical challenges and design principles are introduced in provisions of hardware development, software enlargement and system architectures. Especially radio technologies, energy yielding techniques and cross-layer design for the IWSNs have been discussed [1]. It presents a comprehensive experimental study on the statistical characterization of the wireless channel in different electric-power-system environments, with a 500-kV substation, an industrial power control room, and an secretive network transformer crypt. Field

tests have been perform on IEEE 802.15.4-compliant wireless sensor nodes in real-world power delivery and distribution systems to measure background noise, channel uniqueness, and attenuation in the 2.4-GHz frequency band [2].

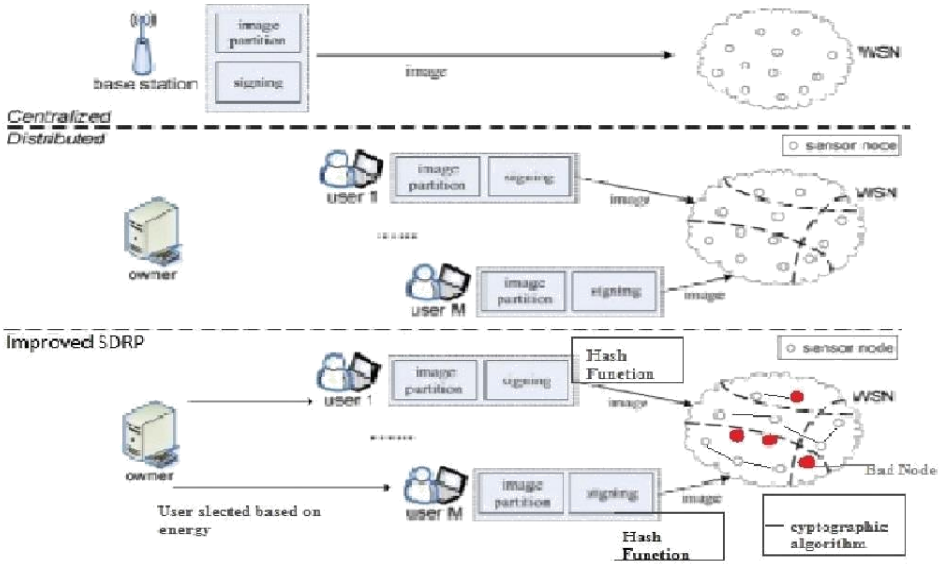

Figure 2. Architecture Diagram

DPDSN [3] stands for Detection of Packet Dropping attacks for wireless Sensor Networks, uses the observation that alternate routing paths are readily available in WSNs, which are typically dense. DPDSN monitors paths and detects whether any node on a path drops packets. Once such an event is detected, it switches to an alternate path for communication. The cost of finding an alternate path is minimized by having it embedded in route discovery of source-initiated and receiver-initiated routing protocols. In distributed probing technique [4], every node in the network will probe the other nodes periodically to detect if any of them fail to perform the forwarding function. Subsequently, node state information can be utilized by the routing protocol to bypass those malicious nodes. In a moderately changing network, the probing technique can detect most of the malicious nodes with a relatively low false positive rate. The packet delivery rate in the network can also be increased accordingly. A resilient packet-forwarding scheme using Neighbor Watch System (NWS) [5], specifically designed for hop-by-hop reliable delivery in face of malicious nodes that drop relaying packets including faulty nodes that fail to relay packets. The scheme basically employs single-path data forwarding that consumes less power than multipath schemes already existing. This scheme converts into multipath data forwarding at the location where NWS detects relaying nodes' misbehavior as the packet is forwarded along the single-path toward the base station. The coordination and communication problems in WSANs are deliberate. They first formulate the mathematical models for the WSANs system. If in that case, a predictor-controller algorithm based on distributed estimation is adopted to mitigate the effects of network-induced delay. At last, they apply a collaborative processing mechanism to meet the desired system requirements and improve the overall control presentation. This approach will group the sensor and actuator nodes to work in parallel so as to reduce the computation complexity and enhance the system reacting time. Simulation outcome demonstrate the effectiveness of our proposed method [6]. Decentralized algorithm is used to calculate the control signals for lights in wireless sensor/actuator networks. This

Algorithm uses a suitable step size in the iterative process used for quickly computing the control signals. Demonstrate the accuracy and efficiency of this approach compared with the by using Mote-based mesh sensor networks. The evaluation error of the new approach is one-eighth as large as that of the penalty method with one-fifth of its computation time [7] to estimating the location of a mobile node based on the range measurements of Cricket sensor network (CSN), where the coordinates of the mobile node are calculated via the method of trilateration. There are, in common, two kinds of obstacles to be tackled and overcome in CSN: One is noisy distance measurements, and the other is the low down data rates of Cricket sensors. To defeat these problems, we propose a fusion prediction-based interacting multiple model (FPB-IMM) algorithm. The FPB-IMM algorithm utilize multiples position measurements produced by trilateration and a self-tuning algorithm; it takes advantage of these multiple measurements to minimize the effect of noisy measurements and the low data rates by modifying a cycle of IMM with fusion prediction[8]. Unlike existing system, our work addressing to provide the efficient security for the reprogramming. Our work relies on predicted aggregated values in an efficient online manner and can complement existing reprogramming to considerably enhance WSN security. Quite recently, He *et al.* have proposed a secure and distributed reprogramming protocol named *SDRP*, which is the first work of its kind. Because a novel identity-based signature scheme is employed in generating public/private key pair of each authoritative user, SDRP is efficient for resource-limited sensor nodes and mobile devices in terms of communication and storage requirements. Moreover, SDRP can achieve all requirements of distributed reprogramming listed in, while keeping the merits of the

well-known mechanisms such. An improvement in SDRP was proposed in [9] In this work, we provide a packet dropper free secure and distributed reprogramming for WSNs with an enhanced random key exchange mechanism proposed in the following section.In this paper, we propose a Distributive Reprogramming of sensor nodes with secure Data Transmission (PDF-SDRP). The proposed work can be split into the following modules that are described in sections that follow. The flow of this system is illustrated in figure 3. Here we also choose the user based on the energy of the WSN so that the Energy of nodes is also improved based on this approach.

A.Network Initialization

Registration of the privileged users to the owners is performed at this stage. The user has the privilege to access its neighbour sensor nodes. The owner allows the user to reprogram without admin involved. The network owner generates public and private key has to be generated for security purpose of the sensor nodes. A random key is generated based on the energy levels of the node and it is used to check the legitimacy of the nodes before selecting them as users.

1) G be a cyclic a group generated by P and G and GT have the same primer order q. Let e = G * G → GT be a bilinear map.

2) Compute the corresponding public key PKown = $s \cdot P$

3) Assume a secure hash functions $H1$ And $H2$, where $H1$ = $\{0, 1\}* \rightarrow$ G and $H2$ =$\{0, 1\}* \rightarrow Zq$

4) Consider Uj be a user identity $UIDj \in \{0, 1\}*$ and public key is $PKj = H1(UIDj\_Prij)$ and private key $SKj = s \cdot PKj$. Now the network owner sends $\{PKj, SKj, Prij\}$ back to Uj using a secure channel

B. User Preprocessing

The network owner set the privilege for the user and calculates the hash value of each packet in the page is added to the packet. The user has to provide signature for overall pages to ensure authentication. The message should contain the reprogramming privileges then targeted node identity set field indicates the identities of the sensor node which the network user wishes to reprogram. Partition the code image and add the signature with the code image.

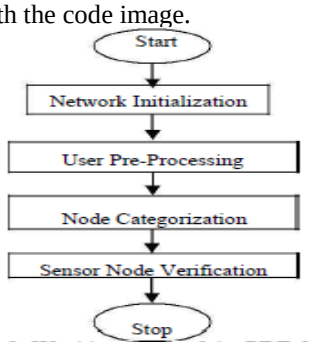

Figure 3. Working Flow of the PDF-SDRP

C.Categorization of the Nodes

The user verify that whether the sensor node have the malicious behavior or not and infected node known as adversaries by using the following procedure.

- It is possible that the infected nodes at time t can spread it to the other nodes
- The final fraction of the infected nodes depends on the classification criterion. It is threshold H here.
- If the value of H is large, then only some nodes will be affected.
- If H is too small all nodes will be infected.

The algorithm used for categorizing good nodes and bad nodes is illustrated in the form of a flow diagram in figure 4. All bad nodes are mostly packet droppers.Let Nf be the number of transmitted packets and Nr be the number of received packets. du be the Droping then

$$du=(Nf-Nr *Nf) Nf+Nr +(Nf* Nf-Nr)$$

Tree-Based Node Categorization Algorithm

1: **Input**: Tree T, with each node u, and its dropping ratio du, threshold value θ, sink node s.
2: **for** every sink node in T **do**
3: find dropping ratio du;
4: **if** $du < \theta$ **then**
5: Set u as *good for sure* or *suspiciously bad;*
6: **if** $du = 0$ **then**
7: Set u as *good for sure;*
8: **else if** $du > 0$
9: Set u as *suspiciously bad*;
10: **else**
11: *break*;
12: **else**
13: Set u as *bad for sure*;
14: **repeat**

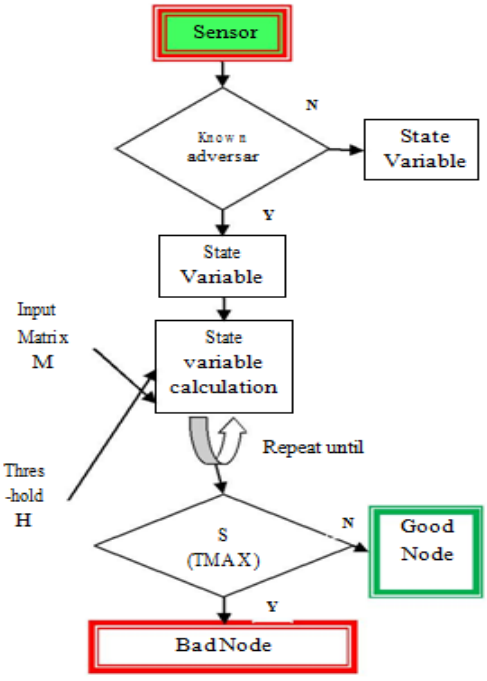

Figure 4. Categorization flow of the Nodes in WSN

D. User Privilege Checking

The sensor node checks the user privilege to analyses the particular user has the privilege to reprogram that sensor node and first pays attention to the legality of the programming privilege and the message. The sensor node checks that, the identity of that particular sensor node is present in the privilege list of the user or not. If it is present in the sense the

system public parameters assigned by the network owner is verified. After the verification the sensor node believes that, the code image is from the authenticated user and the sensor node verifies the data packets in the code image.

E. Random Key Exchange

The wireless sensor network consists of sensor nodes, Users and an Owner. Each and every sensor node in the WSN is initially loaded with the randomly generated key by the Owner.

A single key is generated randomly by using the formula

$$Krandomkey=N*Einitial\%rand\ () \quad (1)$$

After the nodes are loaded with the randomly generated key, all the nodes in the wireless sensor network get the authentication key from its neighbor (i.e.,) the node with one hop distance by sending authentication request packet. That authentication request packet contains the node id, the energy of that node, the distance between that node and its neighbor node. The neighbor node accepts its request and sends the authentication response packet which contains the authentication key along with its ID. That Authentication key is calculated by using the formula

$$AKij=Ej/dij \quad (2)$$

When the source node intends to transmit the data packet, the source node enters into the route discovery phase of AODV for wireless sensor networks. The source node does the following to select the next authenticated forwarder:

- Get the authentication key from its neighbors.
- Neighbor nodes send its authentication code along with its randomly assigned key (Krandomkey).
- The source node check the nodes privilege by analyzing its Krandomkey.
- The source node check the authentication of each of its neighbors.
- The node which has the maximum value of authentication key is selected as next forwarder because authentication key is generated by using the residual energy and the distance.

Thus, by using this scheme we can provide secure routing as well as increase the system throughput too.

F. Energy Consideration

As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable—lack of availability can make the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; thus high availability of these networks is a critical property, and should hold even under malicious conditions. The allocation of the *Users* in SDRP is a significant task as the failure of the User Node might cause the failure of the entire group of nodes under that particular User. Considering the energy of each wireless sensor node the allocation of the users can be done to enhance the overall energy efficiency of the SDRP without altering the multi-authorization of the network.

III. SIMULATION AND ANALYSIS

The simulation is done by using the simulator NS2. Network simulator is a discrete event time driven simulator. NS2 is open source software which uses C++ and Tool Command Language (TCL) for simulation. NS2 is widely used to simulate the networking concepts. The simulation parameters used in the simulation is tabulated below in table 1.

Parameter	Value
Channel Type	Wireless Channel
Radio Propagation model	TwoRayGround
Network interface type	WirelessPhy
MAC Type	IEEE 802.11
Interface Queue Type	PriQueue
Link Layer Type	LL
Antenna Model	Omni Antenna
Routing Protocol	AODV

Table 1. Simulation Parameters

A. Throughput

Throughput is the number of packets successfully delivered over the wireless channel in spite of the interference and other environmental attenuation. The green curve indicates that the PDF-SDRP has greater throughput.

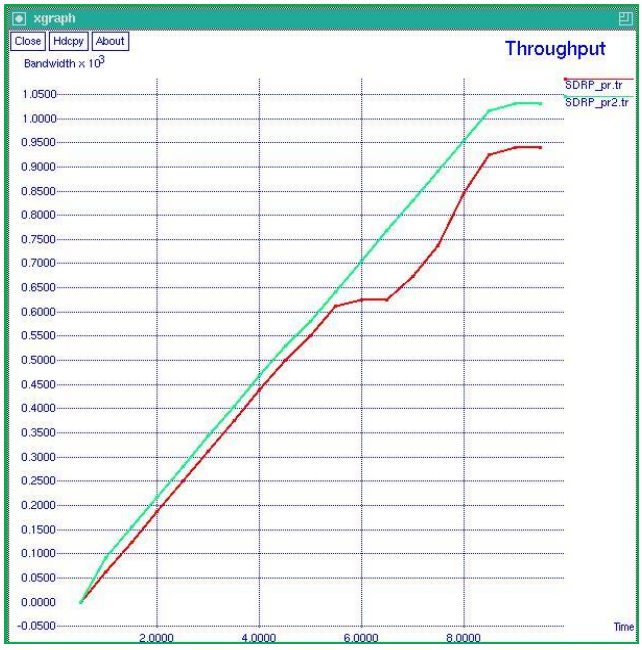

Figure 5. Throughput of SDRP and PDF-SDRP

B. Packet Loss Ratio

Packet Loss is the difference between the number of packets sent by the sender and received at a receiver. The PDF-SDRP shows lower loss than SDRP. In the figure 6, the green curve is the PDF-SDRP and it shows that all the packet droppers are isolated and hence there is lesser loss in the system when compared to the red curve representing SDRP.

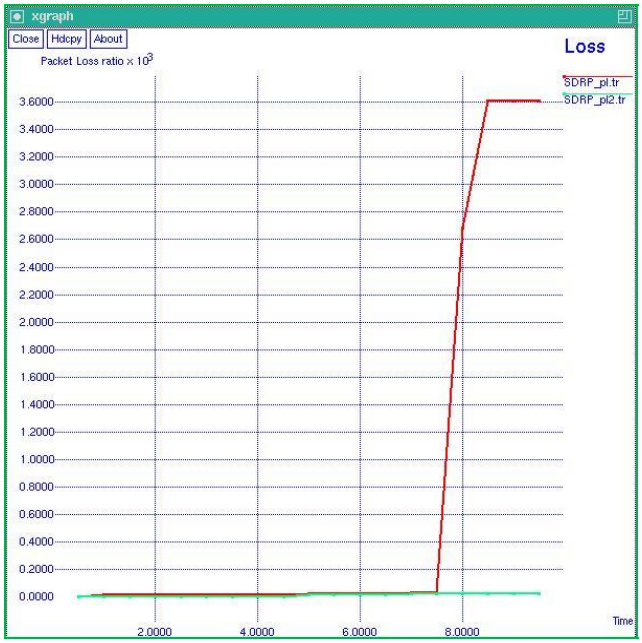

Figure 6. Packet Loss Ratio of SDRP and PDF-SDRP

C. Packet Delay

The packet delay is not as expected due to the fact that the key exchange process is a bit time consuming and hence takes some extra time. However, a tradeoff is present between the delay and the loss.

Figure 7. Packet Delay of SDRP and PDF-SDRP

IV. CONCLUSION

In this paper, a Packet Dropper Free Secure and Distributed Reprogramming Protocol with Random Key Exchange for Wireless Sensor Networks was proposed. The performance analysis was performed using the network simulator to show the efficiency of the system. It in concluded from the analysis provided that the losses can be largely minimized by categorization of the nodes in a WSN as good and bad nodes based on the packet droppers present in the system. The random key exchange mechanism was proposed in this work that improves the quality of service as well as security of the system. Even though some extra delay is caused by the key exchange mechanism the vast difference in terms of loss is a major advantage of this scheme.

REFERENCES

1. V. C. Gungor and G. P. Hancke, “Industrial wireless sensor networks: Challenges, design principles, and technical approaches,” IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.
2. V. C. Gungor, B. Lu, and G. P. Hancke, “Opportunities and challenges of wireless sensor networks in smart grid,” IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.
3. V. Bhuse, A. Gupta, and L. Lilien, “DPDSN: Detection of Packet-Dropping Attacks for Wireless Sensor Networks,”Proc. Fourth Trusted Internet Workshop,2005.
4. M. Just, E. Kranakis, and T. Wan, “Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks,”Proc. Int’l Conf. Ad-Hoc Networks and Wireless (ADHOCNOW ’03),2003
5. S. Lee and Y. Choi, “A Resilient Packet-Forwarding Scheme Against Maliciously Packet-Dropping Nodes in Sensor Net-works,”Proc. Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN ’06),2006.
6. J. Chen, X. Cao, P. Cheng, Y. Xiao, and Y. Sun, “Distributed collaborative control for industrial automation with wireless sensor and actuator networks,” IEEE Trans. Ind. Electron., vol. 57, no. 12, pp. 4219–4230, Dec. 2010.
7. X. Cao, J. Chen, Y. Xiao, and Y. Sun, “Building-environment control with wireless sensor and actuator networks: Centralized versus distributed,” IEEE Trans. Ind. Electron., vol. 57, no. 11, pp. 3596–3604, Nov. 2010.
8. H. Song, V. Shin, and M. Jeon, “Mobile node localization using fusion prediction-based interacting multiple model in cricket sensor network,” IEEE Trans. Ind. Electron., vol. 59, no. 11, pp. 4349–4359, Nov. 2010.
9. Daojing He, Chun Chen, Sammy Chan, Jiajun Bu and Laurence T., “Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks”, Nov 2013.