The Enhanced ECC Approach to Secure Code Dissemination in Wireless Sensor Network

Amritpreet Kaur
Department of Electronics & Communication Engineering
Amritsar, Punjab, India

Guneet Kaur
Department of Electronics & Communication Engineering
Amritsar, Punjab, India

ABSTRACT
Wireless Sensor Networks plays important role in our life so they need to be secured. In this paper we will first give introduction of basics of wireless sensor network and code dissemination technique. We will discuss the impact of reprogramming on WSN in parallel. we will introduce technique called Enhanced ECC to make WSN energy efficient.

Keywords
Reprogramming, Code-dissemination, wireless sensor network, Elliptic curve cryptography.

1. INTRODUCTION
A Wireless Sensor Networks consist of number of nodes that functions to signify data operate data and pass information with each other through radio communication [1].Each sensor node is equipped with different devices like microcontroller, radio, transceiver, antenna and microcontroller. Each node has the tendency to sense data and share data between nodes present in the network [4]. WSNs have various applications ranging from military to forest fire monitoring and security monitoring that makes them so important and valuable. In military WSNs relay secret information that need to be protected from intruders and attackers so security of WSN is a big issue [2].

1.1 Architecture of WSN
In a WSN thousands of nodes are spread over a wide area. The sensor nodes form a network where nodes communicate straight off or indirectly. A WSN consist of a central node called sink node that act as a carriage of all the data from other nodes in the network [4]. The sink node relays this information to the central head office through internet. The network is divided into hardware, an operating system, which addresses the needs of a WSN [4]. In a WSN the nodes are provided with modest battery life so saving the energy of sensor nodes is a big issue that decreases the performance of a WSN. clusters and each cluster has its own cluster head which is a collector [1]. The architecture of a WSN consists of of hardware, an operating system, which addresses the needs of a WSN [4]. In a WSN the nodes are provided with modest battery life so saving the energy of sensor nodes is a big issue that decreases the performance of a WSN.

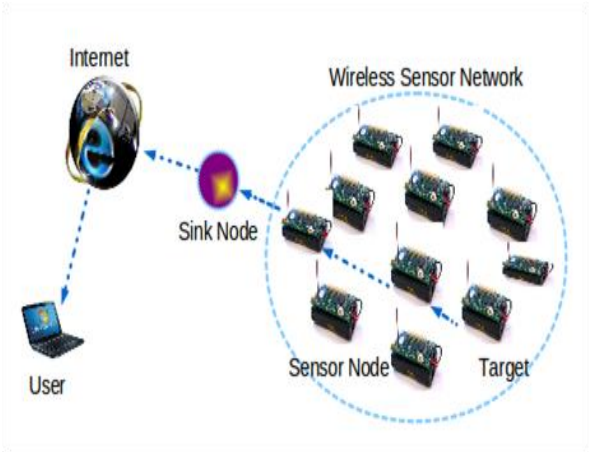


Fig 1: Architecture of a WSN

1.2 Reprogramming in WSN
A wireless sensor network is sometimes needed to be reprogrammed and this is done through wireless links. Reprogramming is done to remove errors, bugs and add new features to the network [3].code dissemination is another term that is used to reprogram the sensor nodes in which new code is spread all over the network. Various code dissemination protocols are available, these protocols help to send new codes through nodes all over the network. Deluge is one such protocol that is being used for efficient propagation of code. It uses epidemic protocol and spatial multiplexing for sending code. Code dissemination faces security challenges in open environment from attackers. The attacker may shoot fake code dissemination packets and force the nodes to pass them thus wasting the restricted battery of nodes [3].

In antagonistic situations where there might be malignant assaults against remote sensor systems, code spread confronts dangers from both outside aggressors and possibly traded off hubs. For instance, the foe may endeavour to alter or supplant the genuine code picture being proliferated to sensor hubs, bringing malevolent code into the sensor organize. As another illustration, the attacker may infuse fake code dispersal parcels and drive ordinary sensor hubs to confirm or potentially forward them, hence debilitating their restricted battery control [3].

2. RELATED WORK
Xiaoyan g Zhong(et.al), 2015 [5] introduced mobile deluge tool which was a mobile network reprogramming tool, Mobile deluge based on Deluge protocol resolved the problems of Deluge and over-the-air reprogramming approach. Mobile deluge had many advantages over deluge; it worked efficiently for heterogeneous WSN and enabled effective code dissemination even over low power WSN

motes. They compared the outcome of Mobile Deluge using lab experiments and real world environment and find out through results that their Mobile deluge approach worked better than Deluge approach.

Zeng Yong (et.al), 2012 [6] proposed a novel code dissemination scheme that used fountain codes to integrate authentication of the network. Deluge based protocols consumed high power and memory, they also causes out-of-delivery problem in packets of wireless sensor networks. Deluge approach was insecure and couldn't defeat DOS attacks. There proposed scheme provided code image privacy, protection against DOS and out-of-delivery packet tolerance.

Daojing He (et.al), 2012, [7], introduced distributed code dissemination protocol called Di-code. A WSN needs to be reprogrammed even in critical environment. The distribution of code to multiple users simultaneously to update the code is sometimes needed, for this the Di-code will work more efficiently. Di-code has the ability to resist Denial-of-service attack. They implemented the proposed approach in practise on a network with low power availability and tested the efficiency of Di-code approach.

Rui Zhang (et.al), 2011, [8], developed a novel approach named LR-seluge, loss-resilent and secure code dissemination scheme. Code dissemination involves removing program bugs and adding new features to wireless sensor network. Code dissemination should be loss and attack resistant even in hostile and vulnerable conditions. They tested the efficiency of proposed LR-seluge through theoretical and simulation analysis and results. Simulation results showed that LR-seluge reduced 40% communication overhead even in hostile conditions with same level of attack.

Joshua Ellul (et.al), 2010, [9] used high level scripts to leverage small update sizes. They translated the scripts to native codes as native codes provided faster execution than larger code at same cost. The transmission of larger code consumed a lot of energy during updating of code in the complete network. The nodes also face high overheads during reprogramming. Native codes on the other hand reduced the overheads and helped in fast transmission of code.

3. PROPOSED METHOD

3.1 Concede Node Formation

This work mainly focuses on enhancing the network for secure Transmission of code distribution .in this system some nodes are separated and these nodes are called approved node. These nodes are placed with system nodes and they are always placed around the Code Distribution Environment. The main function of approved node (Conceded node Cn) is to receive service request from network nodes

3.2 Dynamic Token with ECC

The conceded node will find the document Identification Number of node that is looking for service. After extracting Id the conceded will generate dynamic token with the help of ECC Elliptical curve cryptography algorithm after generating code it will find next node for preferred service . the (Cn) node are used to finds all the preferable nodes for finding suitable path. The conceded nodes stores information of all the sender nodes and then find the next suitable node in route path for secure transmission

The approved nodes which are called as conceded nodes(CN) will find succeeding path of approved nodes for secure routing path .the Cn will generate route for secure message transmission the message transmission will be done with the encryption technique and all message will be encrypted and transmitted to route flow .if network fails in between the transmission. the retransmission of code will start from last conceded node which is stored in route path from which the transmission suspended .instead of starting transmission from the initial position

ALOGRITM: Proposed technique

1: for time=1 to simulation time

2: for i=1:N, where N the number of nodes that placed in the network

3: for CID:, Cn Number of Conceded node

within the route path

4: Find ID number of Cn

5: if location (i) within the loc(Cn);

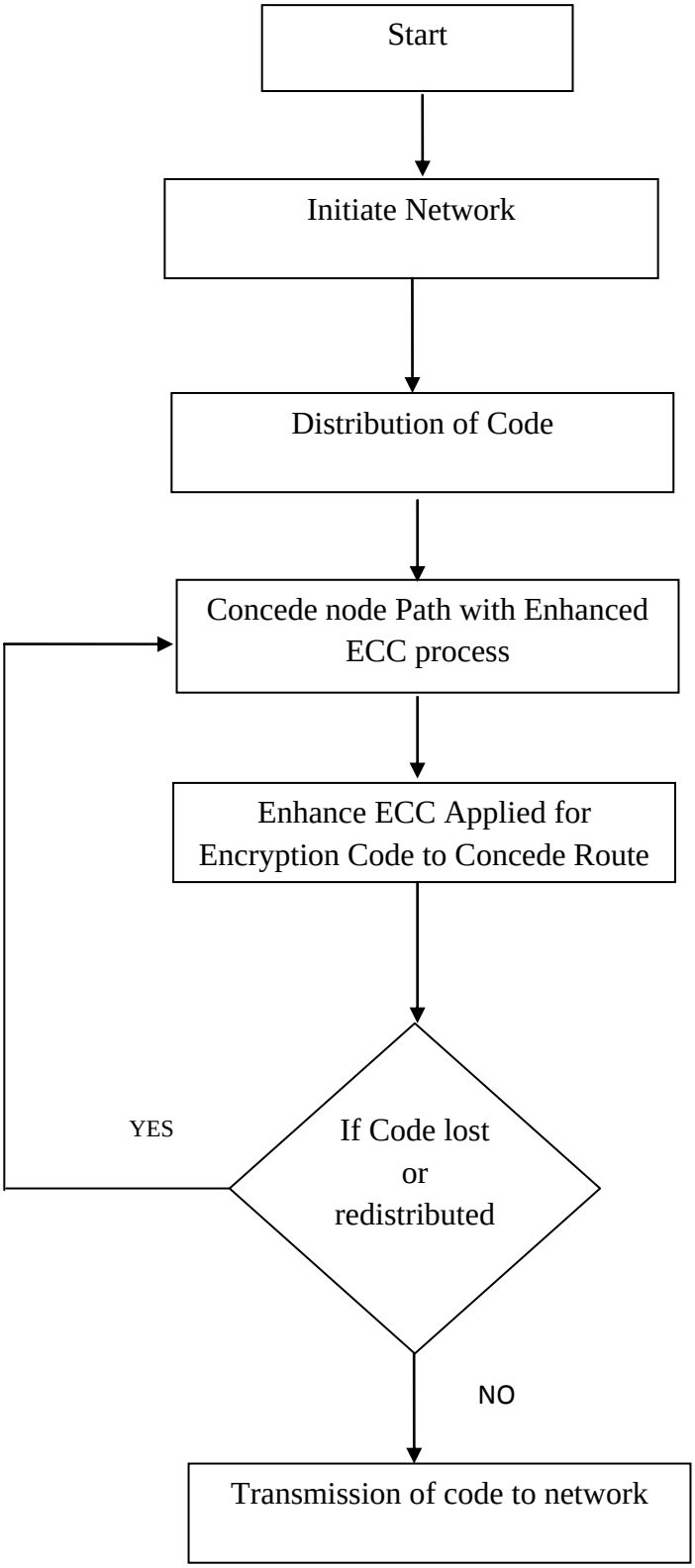
6: Add i to (Cn ID); store information of succeeding concede node in route path

7: end if

8: end

9: end

10: end



4. CONCLUSION

Code Dissemination is used to spread the code over the whole WSN but due to over the air programming the code is vulnerable to attack so ECC is used to protect the data. But using ECC, the network consumes more power so enhanced ECC is used to protect the data with minimum use of energy at the nodes.it provides security protections for code dissemination, including the integrity protection of code. Our proposed technique is superior to all previous attempts for secure code dissemination. Our future work is to test our proposed technique on large environment system with various attacks such as Sybil attack, wormhole attack grey whole attack.

5. REFERENCES

[1] Mrs. B. Chithra, Depavath Harinath,P.Satyanaryana, M.V Ramana Murthy, "Enhancing Security by using ECC Algorithm in Wireless sensor network", IJAIM, Volume-4, Issue1,ISSN 2320-5121, 2015.

[2] Himani Chawla,"Some issues and challenges of Wireless Sensor Networks", Volume 4, Issue 7, July 2014.

[3] Sangwon Hyun, Peng Ning, An Liu North Carolina State University Wenliang Du Syracuse University," Seluge: Secure and DoS-Resistant Code Dissemination in Wireless Sensor Networks", https://discovery.csc.ncsu.edu/pubs/ipsn08-seluge-IEEE.pdf.

[4] Asha Ran Mishra, Mahesh Singh, "Elliptic Curve Cryptography for Security in wireless sensor network", IJERT, ISSN: 2278-0181, Vol-1 issue 3, May-2012.

[5] Xiaoyang Zhong, Miguel Navarro, German Villalba, Xu Liang, Yao Liang, "MobileDeluge: A Novel Mobile Code Dissemination Tool for WSNs", *Mobile Ad Hoc and Senor Systems (MASS) 2014 IEEE 11th International Conference on*, pp. 537-538, 2014.

[6] Jian-Xin Liao, Lei Zhang, Jing-Yu Wang, Min-Yan Liao, Qi Qi, Tong Xu, "Security and efficient data dissemination over wireless sensor network with raptor codes", *Machine Learning and Cybernetics (ICMLC) 2013 International Conference on*, vol. 04, pp. 1596-1600, 2013.

[7] Chun Chen , Sammy Chan , Jiajun Bu, "DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks", IEEE Transactions on Wireless Communications (Volume: 11, Issue: 5, May 2012).

[8] Rui Zhang, Yanchao Zhang, "LR-Seluge: Loss-Resilient and Secure Code Dissemination in Wireless Sensor Networks", *Distributed Computing Systems (ICDCS) 2011 31st International Conference on*, pp. 497-506, 2011, ISSN 1063-6927.

[9] Joshua Ellul, Kirk Martinez, "A Few Bytes are Worth a Thousand Words: Run-Time Compilation of High Level Scripts in Sensor Networks", Distributed Computing Systems Workshops (ICDCSW), 2010 IEEE 30th International Conference.