A Secure Distributed Code Discovery in Wireless Sensor Networks

Sadineni Neelima[1], A.K.Chakravarthy[2]

1,2 Assistant Professor, Department of Information Technology ,
Aditya Engineering College,Surampalem,Kakinada,(India)

ABSTRACT

A wireless sensor network (WSN) consists of little sensor nodes, that is capable of assembling information from the surroundings and communicating to the controller via wireless transceivers. Limited battery energy is employed to control the detector nodes and is extremely troublesome to exchange or recharge it, once the nodes die. It is often difficult or not possible to exchange the batteries of the detector nodes. On the opposite hand, the Base station or Sink is often rich in energy. Since the detector energy is that the most precious resource within the WSN, effective utilization of the energy to improve the network period has been the main focus of abundant of the analysis on the WSN. This can have an effect on the network performance. In most of existing protocols authors considered only on the centralized data dissemination methods without more security and energy consideration. We have a tendency to establish the safety vulnerabilities in previously planned protocols and that we extend the secured and distributed information delivery system with energy concerns. It's the first distributed information discovery and dissemination protocol that permits network owners and approved users to collect information items from detectors without base station and with network life time management. The existing did rip [1] protocol is only concentrating on the security point. In this paper, we propose an enhanced dissemination protocol, which is used to improve the quality of service issues. In the enhanced work, the proposed solution is to enhance the energy efficiency in distributed wireless sensor.

I. INTRODUCTION

The communications within the Wireless Sensor Network (WSN) has the many-to one property, in this data items from a large number of Sensor nodes tend to be targeted into one sinks. Since multi-hop routing is usually required for distant Sensor nodes from the sinks to save huge amount of energy, the devices close to a sink are often loaded with relaying an over-sized quantity of traffic from different nodes. Sensor nodes resources affected in term of energy, processor and memory and dynamic behaviour of ad-hoc communication. The Sensor nodes are commonly expected to work with batteries and they are usually deployed to not easily-accessible or hostile surroundings, generally in large quantities. Routing is a crucial issue in information gathering WSN, whereas on the opposite hand sleep/wake maintenance is that the main problems for event detection networks. Even though, we cannot avoid the failure of nodes, so in our research work, further we added the enhancement with the failure rectification techniques. Our ultimate aim of this project is to provide the energy efficient distributed security system for WSN. And more importantly, all previous data discovery &

dissemination algorithms propose fully centralized method where our method provides data collection scheme in distributed method.

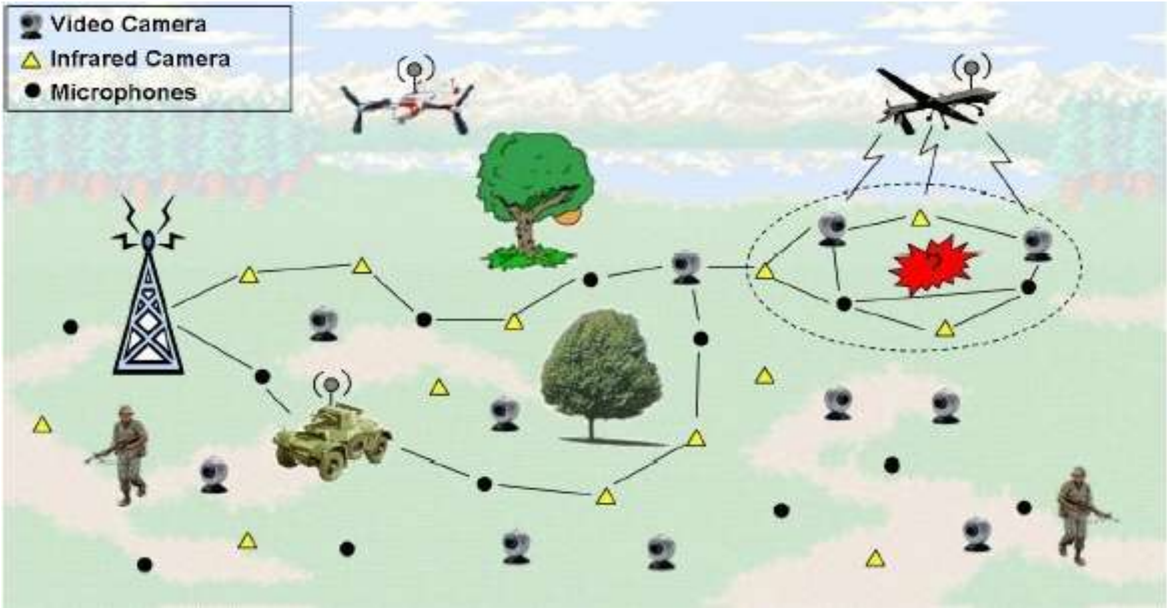


Fig:1.1 Wireless Sensor Network (WSN)

II. LITERATURE SURVEY

A Literature review is a body of text that aims to review the critical points of current knowledge including substantive findings as well as theoretical and methodological contributions to a particular topic. A literature review is a text of a scholarly paper, which includes the current knowledge including substantive findings, as well as theoretical and methodological contributions to a particular topic. Literature reviews are secondary sources, and do not report new or original experimental work. Most often associated with academic oriented literature, such reviews are found in academic journals, while started to do this paper, referred the following papers of integrity checking models in Wireless Sensor Networks and decided to do this project with the existing system, and came to a conclusion that what can be done in the proposed system.

In[1] We present Trickle, an algorithm for propagating and maintaining code updates in wireless sensor networks. Borrowing techniques from the epidemic/gossip, scalable multicast, and wireless broadcast literature, Trickle uses a “polite gossip” policy, where motes periodically broadcast a code summary to local neighbours but stay quiet if they have recently heard a summary identical to theirs. When a mote hears an older summary than its own, it broadcasts an update. Instead of flooding a network with packets, the algorithm controls the send rate so each mote hears a small trickle of packets, just enough to stay up to date. We show that with this simple mechanism, Trickle can scale to thousand-fold changes in network density, propagate new code in the order of seconds, and impose a maintenance cost on the order of a few sends an hour.

In[2] The main problem is that here base station should be involved to distribute the information to the nodes but here it is not happening. So to overcome this problem, Denial of service should be restricted, by allowing base station to give privilege to the users up to some extent so that other users will not be entered to transfer the information. In Wireless Sensor Networks, Code Dissemination is a process of Propagating new code images or commands in the network. Since the WSN are mostly deployed in the military and hostile environments secure code dissemination is needed. Mostly code dissemination protocols are based on two approaches. First one is the centralized approach in which only the base station has the authority to initiate code dissemination. Second one is the distributed

manner means allows multiple authorized network users too simultaneously and directly update code images on different nodes without involving the base station. Motivated by this consideration, we develop a secure and distributed code dissemination protocol named Di Code [2]. A salient feature of Di Code is its ability to resist denial-of-service attacks which have severe consequences on network availability. Di Code in a network of resource limited sensor nodes, which shows the efficiency of our protocol signature verification on the propagation delay of code dissemination in multi hop networks, performance can be improved by using more powerful sensor node. To verify the efficiency of the proposed approach in practice, we also implement the proposed mechanism in a network of resource

constrained sensor nodes.

In[3] Ensuring that every sensor node has the same code version is challenging in dynamic,unreliable multi-hop sensor networks. When nodes have different code versions, the network may not behave as intended, wasting time and energy. We propose and evaluate DHV[5], an efficient code consistency maintenance protocol to ensure that every node in a network will eventually have the same code. DHV is based on the simple observation that if two code versions are different, their corresponding version numbers often differ in only a few least significant bits of their binary representation. DHV allows nodes to carefully select and transmit only necessary bit level information to detect a newer code version in the network.DHV can detect and identify version differences in O (1) messages and latency compared to the logarithmic scale of current protocols. Simulations and experiments on a real MicaZ test bed show that DHV reduces the number of messages by 50%, converges in half the time, and reduces the number of bits transmitted by 40-60% compared to DIP, the state-of-the-art protocol.

In[4] When a sender sends a packet to a receiver, receiver will keep the packet in a buffer. If a buffer is full then the packet is discarded and hence causes a problem. To overcome a problem a technique is used called TESLA. This technique is used by the sender. A packet is sent using a sender MAC value to the packet to the receiver and receiver keep it in buffer. If the sender encloses the packet then receiver will authenticate it so that no loss is there. In this way both sender and receiver get communicated. Multicast technology [4] application has been widely utilized in broadband internet. Source authentication is one of the most needs for many multicast applications transferring real-time information such as stream video and online news. Because multicast current services provided to the group members are changed dynamically, data transferring by a group member is not used by the recipient. In order to verify the identity of the sender who sent the packet and to make sure that the data have not been tampered, an optimized source authentication scheme has been proposed to transfer the authentication information not to the next-door packet. The proposed method for multiple packets authenticates the source with a limited number of electronic signatures. The proposed method can reduce overhead compared to the method by adding a digital signature for every packet. In addition, by sending the generated electronic signature to the first packet and the last packet, it prevents the loss of consecutive packets, as well as a source authentication can be provided in real-time services.

In[5] A data discovery and dissemination protocol for wireless sensor networks (WSNs) is responsible for updating configuration parameters of, and distributing management commands to, the sensor nodes. All existing data discovery and dissemination protocols suffer from two drawbacks. First, they are based on the centralized approach; only the base station can distribute data item. Such an approach is not suitable for emergent multi owner multi-user WSNs. Second, those protocols were not designed with security in mind and hence adversaries can easily launch attacks to harm the network. This paper proposes the first secure and distributed data discovery and dissemination protocol named (Didrip).

We have identified the security vulnerabilities in the data discovery and dissemination when used in WSNs, which have not been addressed in previous research. Also some data A Distributed and Secure Frame Exertion For Data Detection in Wireless Sensor Network 11 discovery and dissemination protocols have been proposed, but none of these approaches support distributed operation. Therefore in this paper, a secure and distributed data discovery and dissemination protocol named Didrip has been proposed. Besides analyzing the security of Didrip, this paper has also reported the evaluation results of Didrip in an experimental network of resource-limited sensor nodes, which shows that Didrip is feasible in practice. We have also given a formal proof of the authenticity and integrity of the disseminated data items in Didrip. Also, due to the open nature of wireless channels, Messages can easily intercept.Thus, in the future work, we will consider how to ensure data confidentiality in the design of secure and distributed data discovery and dissemination protocols.

III. SYSTEM ARCHITECTURE

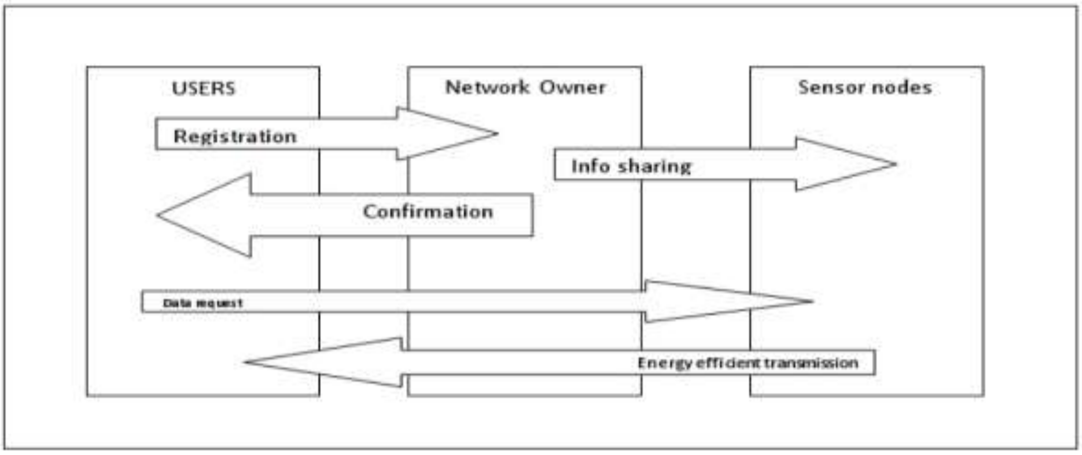
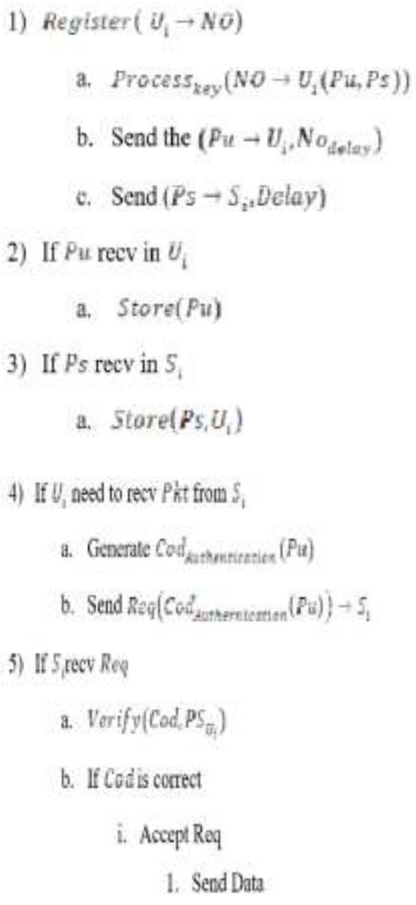


Fig 3.1 Security Architecture

User sends registration request to any interested networks include users address then user has to wait the conformation message from the network owner. After successful registration user can perform Data request operations.Network Owner is responsible for authenticating the user and informs to the sensor nodes about the

Connected nodes.A WSN node contains several technical components. These include the radio, battery, microcontroller, analog circuit, and sensor interface. When using WSN radio technology, you must make important trade-offs. In battery-powered systems, higher radio data rates and more frequent radio use consume more power. Often three years of battery life is a requirement, so many of the WSN systems today are based on ZigBee due to its low-power consumption. The battery life and power management technology are constantly evolving and the availability of IEEE 802.11 bandwidth, Wi-Fi is an interesting technology. The second technology consideration for WSN systems is the battery. In addition to long life requirements, you must consider the size and weight of batteries as well as international standards for shipping batteries and battery availability. The low cost and wide availability of carbon zinc and alkaline batteries make them a common choice. To extend battery life, a WSN node periodically wakes up and transmits data by powering on the radio and then powering it back off to conserve energy. WSN radio technology must efficiently transmit a signal and allow the system to go back to sleep with minimal power use.This means the processor involved must also be able to wake power up, and return to sleep A Secure Distributed Code Discovery in Wireless Sensor Network node efficiently. Microprocessor trends for WSNs include reducing power consumption while maintaining or increasing processor speed. Much like your radio choice, the power consumption and processing speed trade-off is a key concern when selecting a processor for WSNs. This makes the x86 architecture a difficult option for battery-powered devices

A. Software Description :



```
1) $Register(U_i \to NO)$
    a. $Process_{key}(NO \to U_i(Pu, Ps))$
    b. Send the $(Pu \to U_i, No_{delay})$
    c. Send $(Ps \to S_i, Delay)$
2) If $Pu$ recv in $U_i$
    a. $Store(Pu)$
3) If $Ps$ recv in $S_i$
    a. $Store(Ps, U_i)$
4) If $U_i$ need to recv $Pkt$ from $S_i$
    a. Generate $Cod_{Authentication}(Pu)$
    b. Send $Req(Cod_{Authentication}(Pu)) \to S_i$
5) If $S_i$ recv $Req$
    a. $Verify(Cod, PS_{U_i})$
    b. If $Cod$ is correct
        i. Accept Req
            1. Send Data
        c. Else
            i. Reject $Req$
```

Fig 3.2 . Algorithm

IV. RESULTS

Packet Delivery Ratio of Didrip

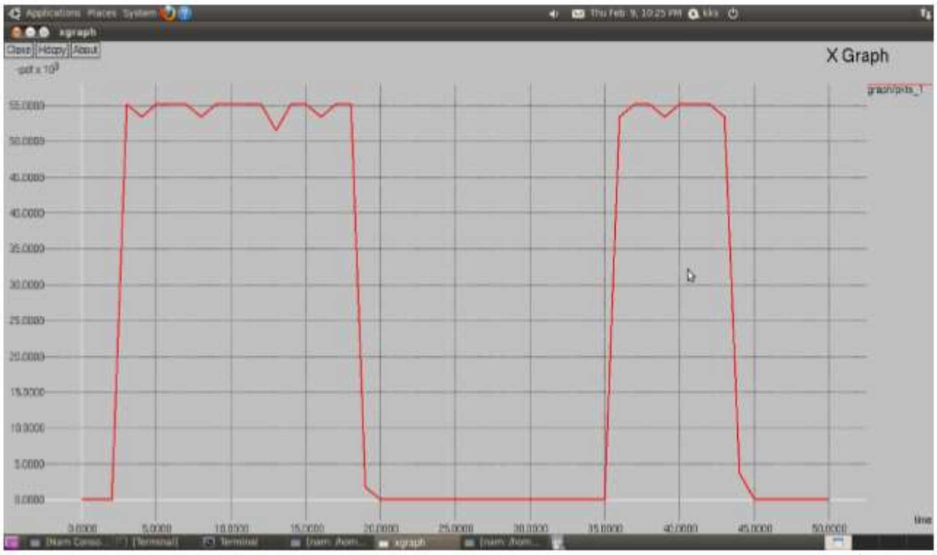


Fig 4.1: Packet Delivery Ratio of Didrip

Here

X axis: time

Y axis: packet delivery ratio

Here DiDrip having very low delay in delivering packets when compared to existence one.

Packet Delivery Ratio of Edidrip

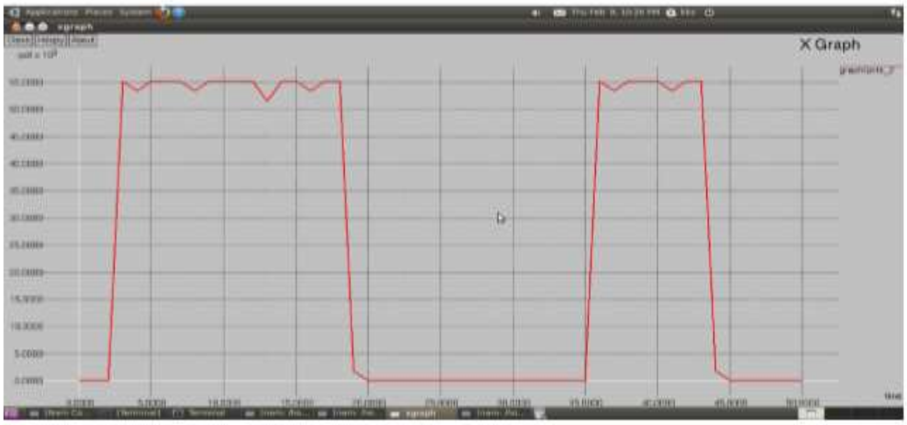


Fig 4.2: Packet Delivery Ratio of EDiDrip

Here

X axis: Time

Y axis: packet delivery ratio

Here EdiDrip is having low delay in delivering packets when compared to DiDrip.

Comparison Between Both DiDrip and EDiDrip

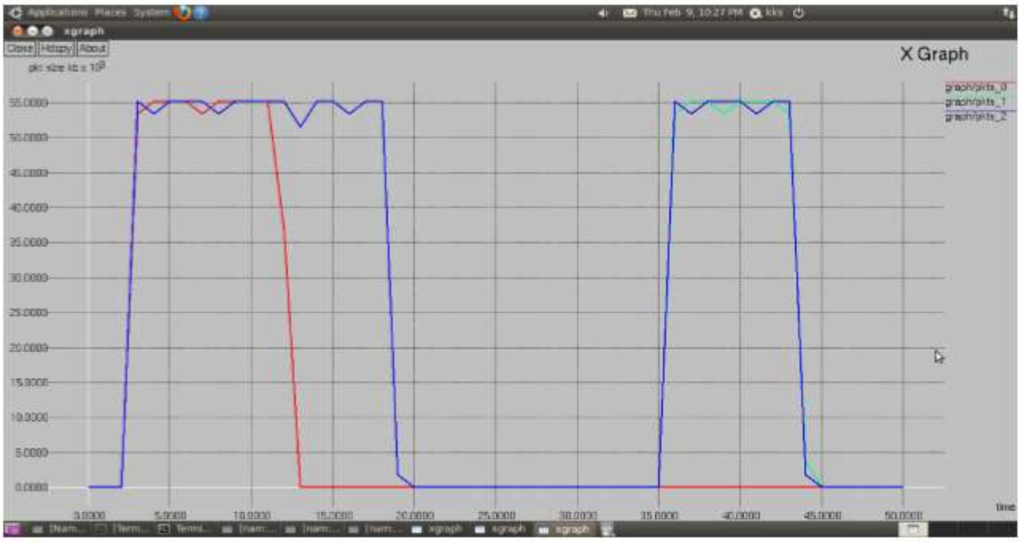


Fig 4.3 Comparision Between Both DiDrip and EDiDrip

Here this graph shows that the comparison of all packets in which Enhanced DiDrip is having less delay.

V. CONCLUSION

In most of existing protocols author considered only on the centralized data dissemination methods without more security and energy consideration. We have proposed the solution to establish the security protocol and that we extended the secured and distributed information delivery system with energy concerns. It's the first distributed information discovery and dissemination protocol that permits network owners and approved users to disperse information items into WSNs without hoping on the base station and with network life time management. From the tested results, the research work providing good energy efficient security architecture to wireless sensor network. In future, this can use autonomous sensor robotic network to improve the disaster management system.

REFERENCES

[1] "Area Flexible (2)Elliptic curve cryptograpy coprocessor", Adnan Abdul"aziz Gutub, CSE dept, King Fahd University of Petroleum and Minerals, SA.

[2] D. He, C. Chen, S. Chan, and J. Bu, "DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks," IEEE Trans. Wireless Communication., vol. 11, no. 5, pp. 1946–1956, May 2012.

[3] T.Dang, N. Bulusu, W. Feng, and S. Park, "DHV: Acode consistency maintenance protocol for multi-hop wireless sensor networks," in Proc. 6th Eur. Conf.Wireless Sensor Netw., 2009, pp. 327–342.

[4] M. Zhao, M. Ma, and Y. Yang, "The Efficient data gathering with mobile collectors and space-division multiple access technique in wireless sensor networks," IEEE Trans. Computer., vol. 60, no. 3, pp. 400–417, Mar. 2011

[5] K. Lin and P. Levis, "Data discovery and dissemination with DIP," in Proc. ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. 2008, pp. 433–444.

[6] T.Dang, N. Bulusu, W. Feng, and S. Park, "DHV: Acode consistency maintenance protocol for multi-hop wireless sensor networks," in Proc. 6th Eur. Conf.Wireless Sensor Netw., 2009, pp. 327–342.

[7] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless Communication, vol. 12, no. 9, pp. 4638– 4646, Sep. 2013.

[8] M. Rahman, N. Nasser, and T. Taleb, "Pairing-based secure timing synchronization for heterogeneous sensor networks," in Proc. IEEE Global Telecommunication Conf., 2008, pp. 1–5.

[9] "designing energy routing protocol with power consumption optimization in manet",
shivashankar1, hosahalli narayanagowda suresh2, golla varaprasad3, and guruswamy
jayanthi4, ieee transactions on emerging topics in computing, 2013.

[10] N. Ahmed, S.S. Kanhere, and S. Jha, "The Holes Problem in Wireless Sensor Networks: A Survey," SIGMOBILE Mobile Computing Comm. Rev., vol. 9, no. 2, pp. 4-18, 2005.

[12] B. Wang, Coverage Control in Sensor Networks. Springer, 2010.

[13] B. Kun, T. Kun, G. Naijie, L.D. Wan, and L. Xiaohu, "Topological Hole Detection in Sensor Networks with Cooperative Neighbours," Proc. Int'l Conf. Systems and Networks Comm. (ICSN'06), p. 31, 2006.