Indian J.Sci.Res. 17(2): 52-525, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

SECURE DATA DISSEMINATION IN WIRELESS SENSOR NETWORKS USING ENHANCED DIDRIP

[1]H. Jayasree, [2]N.Sabitha
[1,2] Department of Computer Science and Engineering, MVSR Engineering College, Hyderabad.

Abstract - Data discovery and dissemination protocols are applied to update configuration parameters & distributed management commands in Wireless Sensor Networks (WSN). Available protocols have two drawbacks: Firstly, they are constructed on centralized procedure; where data items are distributed by only base station and hence this procedure does not support emerging concept of multi-owner-multi-user WSNs. Secondly, these protocols were not built to support security so intruders can easily initiate attacks to harm the network. In this paper, we prefer first secure and distributed data discovery and dissemination protocol known as DiDrip. This enables the network owners to grant multiple network users with different permissions to simultaneously and directly disseminate data items to sensor nodes. The DiDrip protocol is enhanced (EDiDrip) to enhance the network life time in distributed wireless sensor network with pre-failure rectification technique. In this enhanced version of DiDrip protocol we replace a node in case of node failure in order to persist the process of data dissemination. DiDrip is demonstrated as provably secure by extensive security analysis. Our analysis reveals that EDiDrip can solve viable number of security issues that are identified.

Keywords - WSN, Data Dissemination

I. Introduction

A wireless sensor network (WSN) consists of sensor nodes that are capable of assembling information from the surroundings and communicating to the controller via wireless transceivers. The sensor nodes are used to monitor physical and environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. It is necessary to spread data and code through wireless links after the nodes are deployed in WSN in order to adjust parameters of sensors, update the sensor programs or distribute management commands to sensors. This is known as data discovery and dissemination in WSNs. Data discovery and dissemination protocols are implemented in 2 ways: centralized data dissemination and distributed data dissemination process.

In centralized data dissemination process, the data to the sensor nodes can be propagated by only the base station; this does not support emerging concept of multi owner multi user WSNs. These protocols were not designed with security in mind and hence adversaries can easily launch attacks to harm to the network, where as in distributed process data can be disseminated by multiple owners and multiple users.

In case of a centralized architecture of sensor network if the central node or the base station fails, then the entire network will collapse, however the reliability of the sensor network can be increased by using distributed control architecture. Distributed process is adopted in WSNs for the following reasons:

1. Sensor nodes are prone to failure
2. For better collection of data
3. To provide nodes with backup in case of failure of the central node

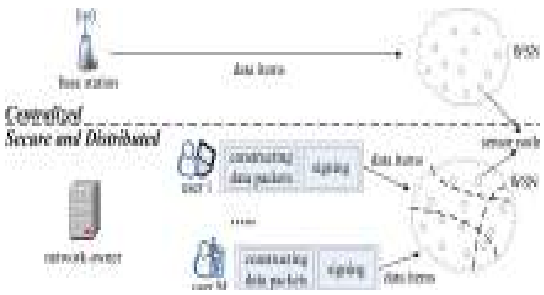

Fig1: Centralized vs Distributed data dissemination

The Fig: 1 shows the comparison between centralized and distributed data dissemination.

In the data dissemination process the centralized approach is inefficient, non-scalable, and vulnerable to security attacks that can be launched anywhere along the communication path. If the central node fails, the entire system will collapse in this approach. Hence there is a need to propose an approach for data discovery and dissemination which works in a distributed scenario. DIDRIP allows the network owners to authorize multiple network users with different privileges and further provide capability to simultaneously and directly disseminate data items into WSNs. It does not rely on base station and provides more security.

II. Review of Data Disssemination protocols in WSN

A. Drip

[1]Corresponding Author

Tolle et al. introduced Sensor Network Management System (SNMS), which is an application-cooperative management system for WSN and Drip [1] is the dissemination protocol that is used in it. Drip is the simplest of all dissemination protocols and is based on Trickle algorithm and establishes an independent trickle for each variable in the data. Drip achieves great efficiency by avoiding redundant transmissions if the same information has already been received by the nodes in the neighbourhood.

Philip Levis et al. [2], presented Trickle, an algorithm for propagating and maintaining code updates in wireless sensor networks, Trickle uses a "polite gossip" policy, where nodes periodically broadcast a code summary to local neighbours but stay quiet if they have recently heard a summary identical to theirs. When a node hears an older summary than its own, it broadcasts an update.

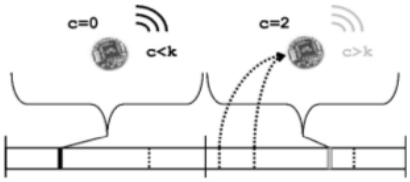

Fig 2: Trickle process

The Fig: 2 represents the trickle process. This process can avoid the repeated transmissions. This process mainly concentrates on the avoidance of repeated information transmission, so there may be a chance of more delay to share new data items. There are no security details for distributed data sharing.

B. CodeDrip

It is a data dissemination protocol proposed by Nildo et al [3]. This protocol is mainly used for dissemination of small values. CodeDrip uses Network Coding to improve reliability, and speed of dissemination by decreasing number of messages transmitted [3]. CodeDrip uses the Trickle algorithm for dissemination. It is similar to Drip except for the fact that here messages are sometimes combined and sent. To combine messages, coding protocols use different operators, here XOR operator is used, which is a Galois field of 2.

C. Dip

DIP (Dissemination Protocol) is a data detection and dissemination protocol proposed by Lin et al. [4]. It is a protocol based on the Trickle algorithm. It works in two parts: detecting whether a difference in data in nodes has occurred, and identifying which data item is different. It uses the concept of version number and keys for each data. DIP, an adaptive dissemination algorithm uses randomized and directed algorithms to quickly find needed updates. The adaptation technique enables DIP to efficiently support disseminating a large number of data items and achieve significant performance.

D. DHV

Thanh Dang et al. authors [5] proposed and evaluated DHV protocol, 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 is 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 different version messages and latency compared to the logarithmic scale of current protocol. This method can successfully discover the data/code difference in the deployed sensor network. It can share the new data items to the network

E. Deluge

J. W. Hui and D. Culler, et al. [1], proposed Deluge for distributing large data objects which are divided into fixed sized pages from source to other nodes over a multi-hop, wireless sensor network. It is reliable and robust when node densities can vary by factors of a thousand or more. This protocol is designed using Trickle algorithm. This process can avoid the repeated transmissions. Every node follows set of strict rules. After a periodic time every node broadcasts the most recent version of the data item it contains, to all those nodes which can listen to its broadcast; other nodes which have received the broadcast will respond with the information available with it. From the information received, node determines which data items should be updated and requests them from any neighbour that advertises the availability of the needed data. Requested data is broadcasted by the nodes receiving these requests. Hence all nodes broadcasts newly received data to all other nodes. Packet losses and attacks are more in this protocol.

II. Data Dissemination through EDIDRIP

A. DIDRIP

DIDRIP stands for distributed data discovery and dissemination routing internet protocol. DIDRIP is 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 by using the autonomous actor placement systems. DIDRIP is an enhanced dissemination protocol, which is used to improve the quality of service issues.

DIDRIP was successfully implemented to increase life time in data dissemination method, since the sensor nodes have limited energy, computation and storage capabilities;

it has become a primary challenge to provide security functions. To provide the security and authentication Merkle hash tree, ECC algorithm and DSA algorithm were applied in DIDRIP protocol. In the EDIDRIP we propose a solution to enhance the network life time in distributed wireless sensor network with pre-failure rectification technique.

B. System Architecture

Fig: 3 shows the system architecture for DIDRIP protocol. In DIDRIP the network owner gives the permission to network users to access data from the sensor devices by registering into the network. The network owner creates its public and private keys, and then loads the public parameters on each node before the network deployment. After that a user gets the dissemination privilege through registering to the network owner. If a user enters the network and wants to disseminate some data items, he/she will need to construct the data dissemination packets and then send them to the nodes. In the packet verification phase, a node verifies each received packet. If the result is positive, it updates the data according to the received packet. ECC security system was applied for user registration and data collection.

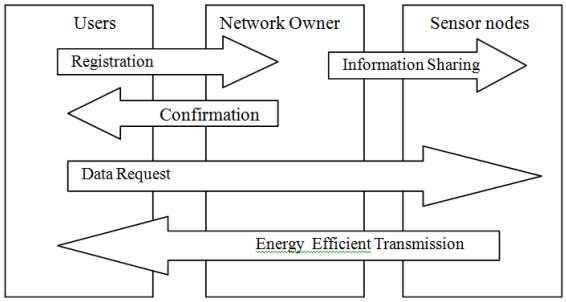

Fig 3: System Architecture

C. DIDRIP Phases

DIDRIP consists of four phases, they are:

1. system initialization phase
2. user joining phase
3. packet pre-processing phase and
4. packet verification phase

In system initialization phase, the network owner creates its public and private keys, and then loads the public parameters on each node before the network deployment. In the user joining phase, a user gets the dissemination privilege by registering to the network owner. In Packet pre-processing phase, if a user enters the network and wants to disseminate some data items, he/she will need to construct the data dissemination packets and then send them to the nodes. In the packet verification phase, a node verifies each received packet. If the result is positive, it updates the data according to the received packet.

IV. Results and Analysis

A. Implementation and Experimental Setup

We have tested our simulation output with NS2 simulator. To analyze the performance we have compared the results of data dissemination in WSN through Centralized approach, DIDRIP and EDIDRIP. In order to evaluate the Centralized method, DIDRIP and EDIDRIP methods the network setup was executed by increasing the number of nodes from 15 to 50, 50 to 200, 200 to 500, 500 to 750 and 750 to 1000 nodes. Performance of each protocol was executed with respect to the following parameters.

Packet delivery fraction

This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source.

Delay

This is defined as the average time taken for a packet to be transmitted from the source to the destination

Throughput

This is defined as the total amount of data that the destination receives from the source divided by the time which takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. And finally overall picture of performance of each protocol is depleted considering all cases respectively.

Figs: 4 & 5 illustrate the results of data dissemination through Centralized approach & DIDRIP which clearly demonstrate that in centralized approach the packets are sent from the network owner (node represented in purple colour) to the user from the sensor nodes, whereas in DIDRIP the packets are sent from the sensor nodes to the users directly with out relaying on the network owner.

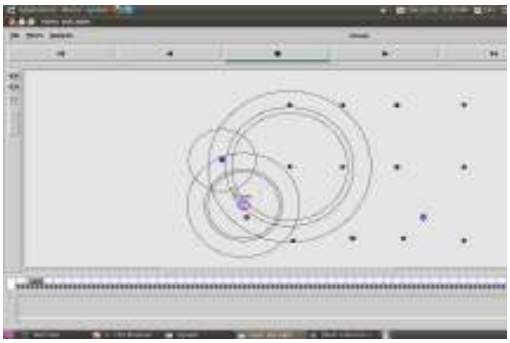

Fig 4: Data dissemination process by using centralized method

Fig 5: Data Dissemination Process By Using DIDRIP Protocol

In the enhanced work EDIDRIP to demonstrate that there is improvement in the network life time in distributed wireless sensor network we consider pre-failure rectification technique by replacing a node in case of node failure in order to persist the process of data dissemination. The results of EDIDRIP are shown in Figs: 6 to 8. Fig: 6 illustrates the case where a node fails and the failure node is represented in the red colour node. The failure of node is identified in advance and exchanges the node by the network owner. Figs: 7 and 8 show the rectification technique by replacing the failure node with another sensor node. The red colour node is replaced by another sensor node.

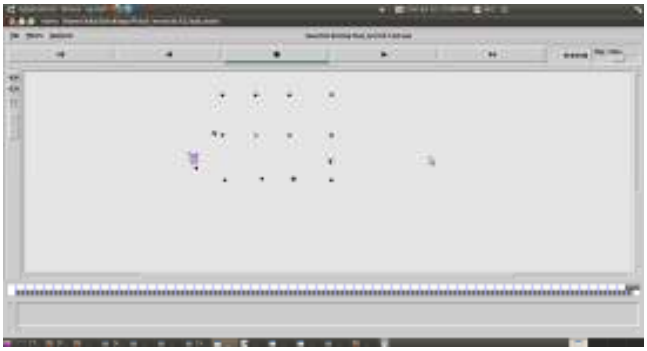

Fig 6: Scenario of node failure

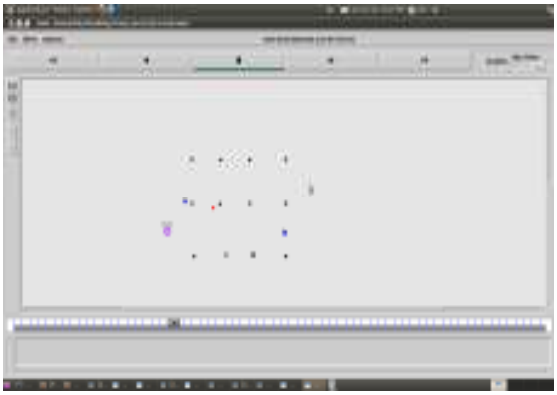

Fig 7: Scenario of node replacement diagram

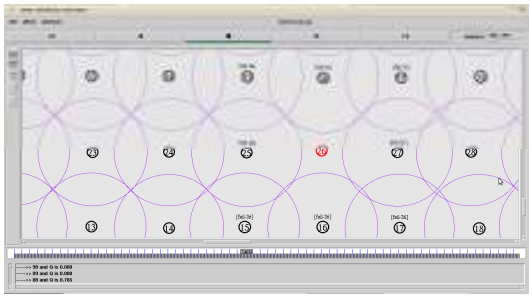

Fig 8: shows the Failure detection and replacement system

B. **Comparison of Centralized, DIDRIP &EDIDRIP**

In order to evaluate the Centralized method, DIDRIP and EDIDRIP methods the network setup was executed by increasing the number of nodes from 15 to 50, 50 to 200, 200 to 500, 500 to 750 and 750 to 1000 nodes. Performance of each protocol was executed with respect to the following parameters: delay, throughput and packet delivery ratio.

Delay:

Delay is proportional to number of nodes. Delay increases as the number of nodes increase. Delay is high in centralized method it is reduced by using DIDRIP and EDIDRIP protocols. Table 2 displays the result add Fig: 9 show the performance of 3 protocols for delay parameter.

Table 2: Performance of Centralized, DIDRIP, and EDIDRIP methods for delay parameter

Number of Nodes	CENTRALIZED (seconds)	DIDRIP (seconds)	EDIDRIP (seconds)
15	0.413372	0.018513	0.016071
50	0.431134	0.069445	0.065642
100	0.431186	0.125101	0.11669
200	0.438299	0.127272	0.128585
500	0.44121	0.13108	0.128661
750	0.442152	0.275211	0.272778
1000	0.448157	0.285716	0.28578

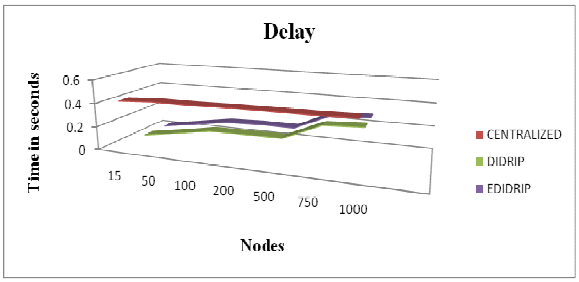

Fig 9: Performance of Centralized, DIDRIP, and EDIDRIP methods for delay parameter

Packet Delivery Fraction:

PDF decreases as the number of nodes in the network increases. PDF is high in DIDRIP and EDIDRIP protocols. Table 3 displays the result and Fig: 10 show the performance of 3 protocols for PDF parameter.

Table 3: Performance of Centralized, DIDRIP, and EDIDRIP methods for packet delivery parameter

Number of Nodes	Centralized (PDF %)	DIDRIP (PDF %)	EDIDRIP (PDF %)
15	60.251	99.721	99.72161
50	60.158	98.627	98.92465
100	60.01484	97.629	97.86848
200	60.00161	91.49233	92.18766
500	59.6234	93.16556	93.16597
750	59.26386	94.12449	94.42259
1000	58.201	91.31285	91.38216

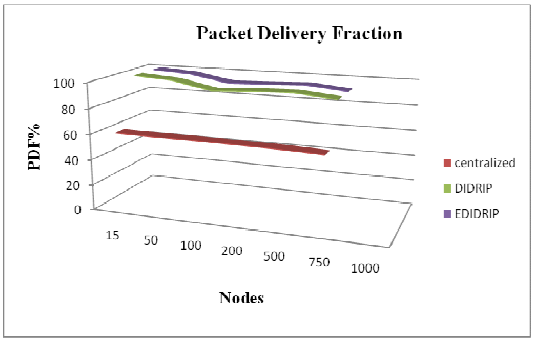

Fig 10: Performance of Centralized, DIDRIP, and EDIDRIP methods for packet delivery parameter

Throughput:

The throughput is increased by using DIDRIP and EDIDRIP protocol and it is very less in centralized method. Table 4 displays the result and Fig: 11 show the performance of 3 protocols for PDF parameter.

Table 4: Performance of Centralized, DIDRIP, and EDIDRIP methods for throughput

Number of Nodes	Centralized (bits/seconds)	DIDRIP (bits/seconds)	EDIDRIP (bits/seconds)
15	8280	20556.25	20556.50
50	8251.25	20125	20153
100	8251.5	18860	19003.78
200	8193.75	19205	19025
500	8222.5	19406.25	19406.25
750	8235.45	19505.3	19756.32
1000	8240.3	18831.25	18831.28

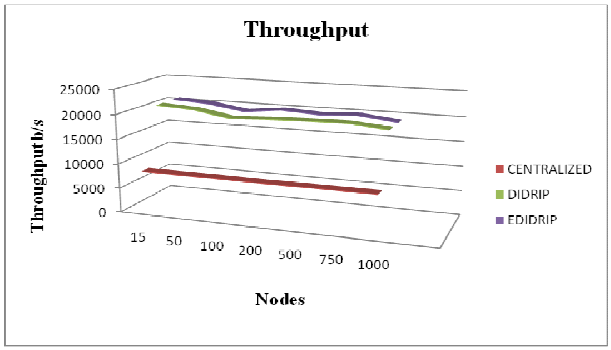

Fig 11: Performance of Centralized, DIDRIP, and EDIDRIP methods for throughput

Conclusion And Future Work

Wireless Sensor Networks is a wide and open area in networking research, which is increasingly being deployed for monitoring applications. This demands the need for quickly and efficiently disseminating data to sensor nodes to reprogram them to suite the current needs of the application. We experimented EDIDRIP protocol, 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 results obtained, we conclude that the EDIDRIP protocol provides good energy efficient security architecture to wireless sensor network.

The efficiency and security can be improved by adding additional mechanisms to ensure data confidentially in the design of secure and distributed data discovery and dissemination routing internet protocol.

References

[1] Akyildiz, I.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks. IEEE Commun. Mag. 2002, 40, 102–114.

[2] Tubaishat, M.; Madria, S. Sensor networks: an overview. IEEE Potentials 2003, 22, 20–30.

[3] Hac, A. Wireless Sensor Network Designs. John Wiley & Sons Ltd: Etobicoke, Ontario, Canada, 2003. Sensors 2009, 9 6894

[4] Raghavendra, C.; Sivalingam, K.; Znati, T. Wireless Sensor Networks. Springer: New York, NY, USA, 2004.

[5] Sohrabi, K.; Gao, J.; Ailawadhi, V.; Pottie, G. Protocols for self-organization of a wireless sensor network. IEEE Personal Commun. 2000, 7, 16–27.

[6] Culler, D.; Estrin, D.; Srivastava, M. Overview of sensor networks. IEEE Comput. 2004, 37, 41–49.

[7] Rajaravivarma, V.; Yang, Y.; Yang, T. An Overview of Wireless Sensor Network and Applications. In Proceedings of 35th Southeastern Symposium on System Theory, Morgantown, WV, USA, 2003; pp. 432–436.

[8] Verdone, R.; Dardari, D.; Mazzini, G.; Conti, A. Wireless Sensor and Actuator Networks; Elsevier: London, UK, 2008.

[9] Verdone, R. Wireless Sensor Networks. In Proceedings of the 5th European Conference, Bologna, Italy, 2008.

[10] Culler, D.; Estrin, D.; Srivastava, M. Overview of sensor networks. IEEE Comput. Mag. 2004, 37, 41–49.

[11] Basagni, S.; Conti, M.; Giordano, S.; Stojmenovic, I. Mobile Ad Hoc Networking; Wiley: San Francisco, CA, USA, 2004.

[12] IEEE 802.15.4 Standard. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs); IEEE: Piscataway, NJ, USA, 2006.