International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 3, Issue 6, June 2016)

Performance Analysis of Secure data distribution in Wireless Sensor Networks

Geeta
Department of Computer Network & Engineering
PDACE, Kalaburagi, Karnataka, India
geetpatil044@gmail.com

Shridevi Soma
Department of Computer Science & Engineering
PDACE, Kalaburagi, Karnataka, India

***Abstract* – A data discovery and dissemination protocol for wireless sensor networks (WSNs) is responsible for updating configuration parameters 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 items. 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 a first secure and distributed data discovery and dissemination protocol named DiDrip. It allows the network owners to authorize multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes. Moreover, as demonstrated by the theoretical analysis, The proposed system addresses a number of possible security vulnerabilities were identified. Extensive security analysis show DiDrip is provably secure, Hence DiDrip is implemented ,in an experimental network of resource-limited sensor nodes to show its high efficiency in practice**

***Index Terms* – DiDrip, DHV, DIP, Hash Key, ECDSA, WSN.**

I. INTRODUCTION

A wireless sensor network (WSN) consists of a collection of these nodes that have the facility to sense, process data and communicate with each other via a wireless connection. The improvement in sensor technology has made it possible to have very small, low powered sensing devices equipped with programmable compute, multiple parameter sensing and wireless message capability. Also the low cost makes it possible to have a network of hundreds or thousands of these sensors, thereby enhancing the consistency and accuracy of data and the area coverage. Wireless sensor networks offer information about isolated structures, wide-spread environmental changes, etc. Wireless sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental situation,

In this paper, A secure and data discovery and dissemination protocol (DiDrip) has been proposed. DiDrip consists of four phases, [1] system initialization, [2] user joining, [3] packet preprocessing [4] packet verification. For the basic protocol, 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 through registering to the network owner. In packet preprocessing 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. such as sound, temperature, and motion.

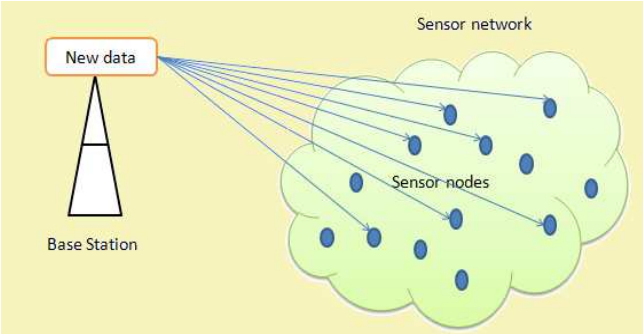

Fig 1. Dissemination process in WSN

The Proposed work is organized in 6 sections. Section 1 presents a general introduction of Wireless sensor network and network. Section 2 presents the related work of the different types of protocol. Section 3 presents the design of the proposed system. Section 4 presents Results and Discussion. Section 5 includes performance analysis Section 6 concludes the work with future enhancement of the proposed system.

II. RELATED WORK

The main objective of the authors [1] J. W. Hui is to analyse a reliable data dissemination protocol for propagating large data objects from one or more source nodes to many other nodes over a multihop, wireless sensor network. Deluge builds from prior work in density-aware, epidemic maintenance protocols. Using both a real-world deployment and simulation, auhtors show that Deluge can reliably disseminate data to all nodes and characterize its overall performance. On Mica2-dot nodes, Deluge can push nearly 90 bytes/second, one-ninth the maximum transmission rate of the radio supported under TinyOS. Control messages are limited

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 3, Issue 6, June 2016)

to 18% of all transmissions. At scale, the protocol exposes interesting propagation dynamics only hinted at by previous dissemination work. A simple model is also derived which describes the limits of data propagation in wireless networks. Finally the rates obtained for dissemination are inherently lower than that for single path propagation. It appears very hard to significantly improve upon the rate obtained by Deluge and i establishing a tight lower bound as an open problem

The new protocol DiCode is proposed by [2] D. He, C. Chen, S. Chan and J. Bu .Code dissemination in a wireless sensor network (WSN) is the process of propagating a new program image or relevant commands to sensor nodes. As a WSN is usually deployed in hostile environments, secure code dissemination is and will continue to be a major concern. Most code dissemination protocols are based on the centralized approach in which only the base station has the authority to initiate code dissemination. However, it is desirable and sometimes necessary to disseminate code images in a distributed manner which allows multiple authorized network users to simultaneously and directly update code images on different nodes without involving the base station. Motivated by this consideration, they developed a secure and distributed code dissemination protocol named DiCode. A salient feature of DiCode is its ability to resist denial-of-service attacks which have severe consequences on network availability. Further, the security properties of Dicode protocol are demonstrated by theoretical analysis. To verify the efficiency of the proposed approach in practice, the proposed mechanism in a network of resource-constrained sensor nodes.

DHV (Difference detection-Horizontal search-Vertical search) [3] is a code consistency maintenance protocol given by Dang et al, 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.

DIP (Dissemination Protocol) is a data detection and dissemination protocol proposed by [5] Lin et al.. Prior approaches, such as Trickle or SPIN, have overheads that scale linearly with the number of data items. For T items, DIP can identify new items with O(log(T)) packets while maintaining a O(l) detection latency. To achieve this performance in a wide spectrum of network configurations, DIP uses a hybrid approach of randomized scanning and tree-based directed searches. By dynamically selecting which of the two algorithms to use, DIP outperforms both in terms of transmissions and speed. Simulation and testbed experiments show that DIP sends 20-60% fewer packets than existing protocols and can be 200% faster, while only requiring O(log(log(T))) additional state per data item.

The primary challenge of providing security functions in WSNs is the limited capabilities of sensor nodes in terms of computation, energy and storage. For example, to provide authentication function to disseminated data, a commonly used solution is digital signature. That is, users digitally sign each packet individually and nodes need to verify the signature before processing it. However, such an asymmetric mechanism incurs significant computational and communication overhead and is not applicable to sensor nodes. To address this problem, TESLA and its various extensions have been proposed [7], [6], which are based on the delayed disclosure of authentication keys, i.e., the key used to authenticate a message is disclosed in the next message. Unfortunately, due to the authentication delay, these mechanisms are vulnerable to a flooding attack which causes each sensor node to buffer all forged data items until the disclosed key is received.

Another possible approach to authentication is by symmetric key cryptography. However, this approach is vulnerable to node compromise attack because once a node is compromised, the globally shared secret keys are revealed.

From the survey work we concluded that none of the protocols provide the security to the sensor nodes if there is no security, sensor nodes can receive data from unauthorised nodes , unauthorised nodes sends the bogus and unwanted data and so it is a time consuming processs and all are based on centralized approach only base station sends data to the sensor nodes if the base station is fails there is no communication between nodes. so we proposed a DiDrip is a distributed and security protocol.

III. PROPOSED WORK

Fig 2 shows the System Architecture of distributed network . For our basic protocol, 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 through registering to the network owner. In packet preprocessing 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.

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 3, Issue 6, June 2016)

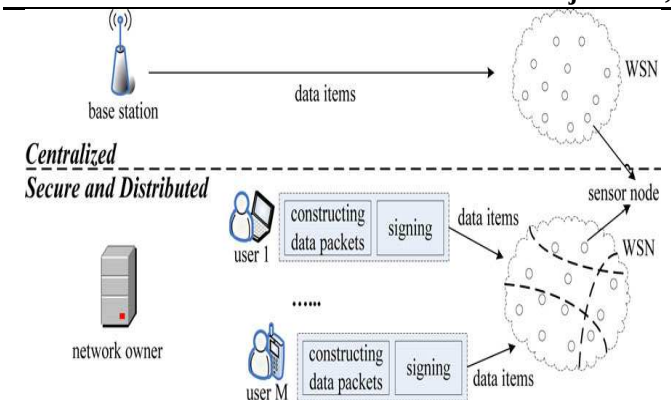

Fig 2. System Architecture

1) System Initialization Phase

In this phase, The network owner carries out the following steps to derive a private key and some public parameters. it then selects the private key and computes the public key. After that, the public parameters are preloaded in each node of the network

2) User Joining Phase

This phase is invoked when a user with the identity UID, hopes to obtain privilege level. User chooses the private key and computes the public key. Then user sends a UID to the network owner, where Prij denotes the dissemination privilege of user. Upon receiving this message, the network owner generates the certificate.

3) Packet Pre-Processing Phase

Similarly, the network owner assigns a pre-defined key to identify this advertisement packet. With the method of Merkle hash tree, user builds a Merkle hash tree from then data items in the following way. All the data items are treated as the leaves of the tree. A newset of internal nodes at the upper level is formed; each internal node is computed as the hash value of the concatenation of two child nodes. This process is continued until the root node is formed, resulting in a Merkle hash tree with depth log Before disseminating the n data items,user signs the root node with his/her private key and then transmits the advertisement packet comprising user certificate Subsequently, user disseminates each data item along with the appropriate internal nodes for verification purpose. Note that as described above, user certificate contains user identity information UID and dissemination privilege Prij. Before the network deployment, the network owner assigns a pre-defined key to identify this advertisement packet.

4) Elliptic Curve Digital Signaure Algorithm(ECDSA)

Digital signatures are somesome big integers ,such as long strings of 1024 bits.It can be sent b sender ,others cannot fake it.once receiver obtain the signature,sender cannot den transmitting ,if others Fake the signature the receiver can Compare it by gaining the message integrity

5) Signature Generation

Step 1: Select a random k in [1, n - 1].
Step 2: Calculate a curve point k*G=(x1,y1)
Step 3: Calculate 1 $r = x1 \ mod \ n$. If $r = 0$, then go back to step 1.
Step 4: Calculate $e = SHA\text{-}1(m)$.
Step 5: Calculate $s = (e + k + rd) \ mod \ n$. If $s = 0$, then go back to step 1.
Step 6: Send the message m and digital signature (r, s)

6) SignatureVerification

To verify message and signature(r,s) we should do the followings

Step 1: Verify that r and s are integers in[1, n - 1]. If not, the signature in invalid.
Step 2: Calculate $e = SHA-1(m)$.
Step 3: Calculate 1 $w \ s \ mod \ n - =$.
Step 4: Calculate1 $u1 =(e \times w) \ mod \ n$, u2 $u =(r \times w \ )mod \ n$.
Step 5: Calculate the curve point $X = u1 \ G + u2 \ Q = (x1, y1)$
Step 6: If $X = O$, the signature is invalid, and refuses it. Else calculate $v = x1 \ mod \ n$.
Step 7: Bob will accept the signature if and only if $v= r$.

7) Packet Verification Phase

When a sensor node, say, receives a packet either from an authorized user or from its one-hop neighbours, it first checks the packet's key field. Comparing the two methods, the data hash chain method incurs less communication overhead than the Mer-kle hash tree method. In the data hash chain method, only one hash value of a packet is included in each packet. On the contrary, in the Merkle hash tree method, D(the tree depth) hash values are included in each packet. However, a limitation of the data hash tree method is that it just works well in networks with in-sequence packet delivery. Such a limitation does not exist in the Merkle hash tree method since it allows each packet to be immediately authenticated upon its arrival at a node. Therefore, the choice of each method depends on this characteristic of the WSNs.

8) Performance Analysis:

For the proposed system , we use the Following specific measurements to evaluate its performance:

- Packet Delivery Ratio
- End-to-End Delay
- Packet Loss Ratio

The following flow diagram explains about projrct execution and how the information will transfers in the network. The flow consist of four phases in phase 1 system set up the parameters like no of nodes taken distance between the each nodes routing protocol(AODV), no of nodes and Queue length and linl layer parameter adjustment ,simulation time .after setting the parameters network owner creates its public and private keys. in phase 2 user will joins the network by registering dissemination privileges through network owner

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 3, Issue 6, June 2016)

.phase 3 is the packet preprocessing user node constructs the data packets in last phase 4 packet verification sensor node verifies each packets by comparing the certificate key generated by the owner node and user sent data (key, data, cert) ,if both signatures valid then sensor receives packets otherwise its rejects packets

IV. RESULT ANALYSIS

A simulation model based on NS2 is used, assumed that the dimension of the scenario as1000x100m in that 43 wireless node randomly deployed. Each wireless nodes initials energy is 3.4j, 10 Mbps bandwidth and each packet size 512 kbps. A two way propagation model is assumed by radio model. We have considered a network topology consisting of 43 nodes and 25 different data variables are disseminated.

The new protocol is found to resist cases of pollution attacks i.e. only valid data packets are received and processed by the intermediate nodes in the network. Also immediate authentication of packets is achieved using certificate value generate by owner node and stored in the data packets transmitted.

Parameter	Setup
set Val (Chan)	Channel/Wireless Channel
set Val(prop)	Propagation/Two Ray Ground
set Val(net if)	Wireless Physical
set Val(Mac)	Mac/802_11
set Val(if q)	Queue/Drop Tail/Pri Queue
set Val(LL)	LL
set Val(ant)	Antenna/Omni Antenna
set queue length	50
set Val(nun nodes)	7
set Val(routing protocol)	AODV
set Val(x)	1131
set Val(y)	909
set Val(stop)	20

Table 1 .simulation parameters

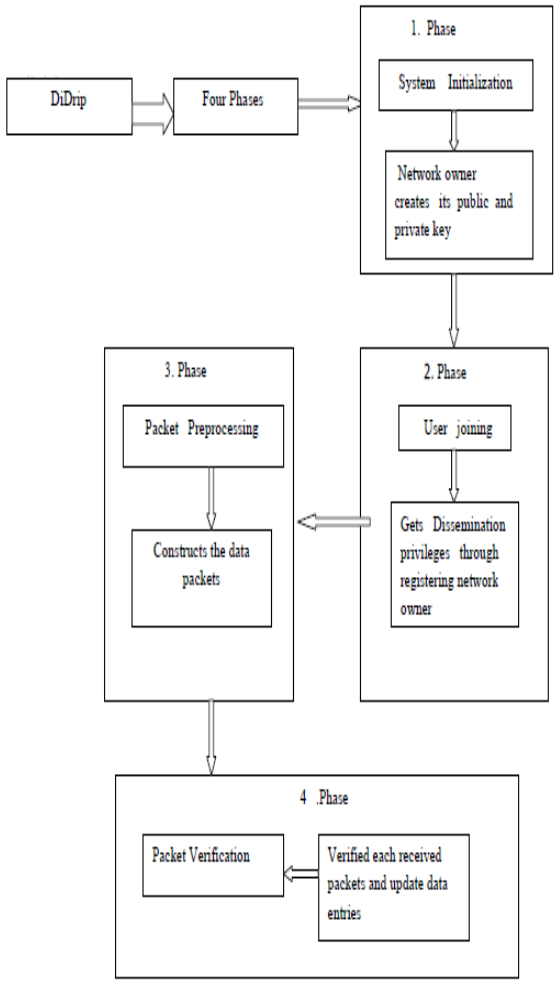

Fig 3. Information processing flow in DiDrip

According to the basic protocol of DiDrip, user Uj generates its public and private keys and sends a 3-tuple UIDj; Prij; PKj > to the network owner. When the network owner receives the 3-tuple, it no longer generates the ertificate Certj. Instead, it signs the 3-tuple with its private key and sends it to the sensor nodes. Finally, each node stores the 3-tuple . The user certificate Certj stored in packet P0 is replaced by UIDj. according to the received identity UIDj, node Sj first picks up the dissemination privilege Prij from its storage and then pays attention to the legality of Prij. If the result is positive, node Sj uses the public key PKj from its storage to run an ECDSA verify operation to authenticate the signature; otherwise, node Sj simply discards the packet. Note that node Sj does not need to authenticate the certificate the public- key/dissemination-privilege pair <UIDj; Prij; PKj > of each network user is just 2 + 6 + 40 = 48 bytes. Therefore, assuming the protocol supports 500 network users, the code size is about 23 KB. We consider the resource-limited sensor nodes such as TelosB motes as examples. The 1-MB Flash memory is enough for storing these public parameters.

The below two graphs describes end to end delay between two nodes and packet loss beween nodes.compare to the previous protocols no of packet loss is reduced,in the previous work delay occurs at the starting of transmission in DiDrip protocol delay is occurs exponionally almost reduced.

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 3, Issue 6, June 2016)

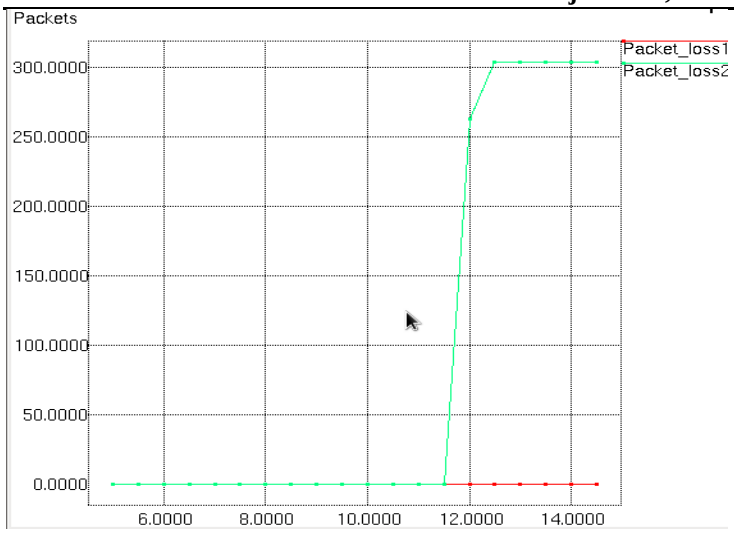

Fig 4.Pocket loss between nodes 1 and 2

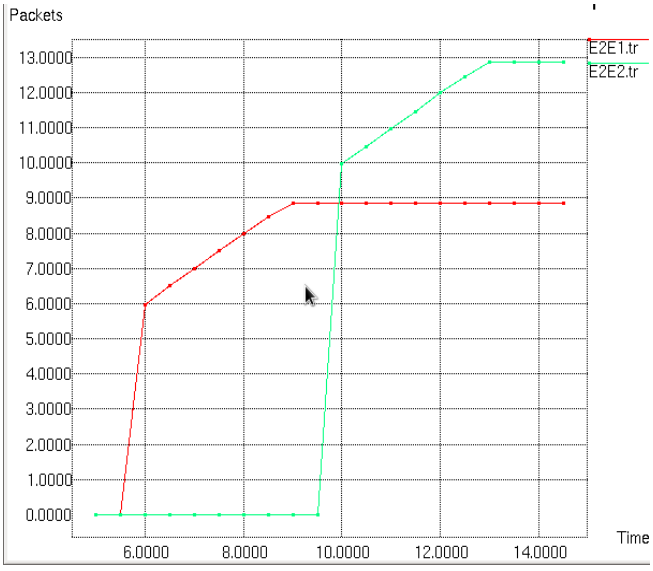

Fig 5.End to End Delay between nodes 1 and 2

V. SECURITY AND PERFORMANCE ANALYSIS

First we perform and analyze the security offered by this protocol.

1. Resistance to pollution attacks- Attackers can't pollute the network with bogus data since data transfer done is always verified using hash techniques
2. Resistance to Denial-of-Service attacks- Immediate authentication of packets is done at each destination, so bogus packets can be discarded and only valid packets pass through
3. Real time key generation- No-pre stored keys in nodes; they are calculated at time of data transfer only.
4. No single point of failure more then one owner node can be created
5. Compare to previous protocol Didrip is secure protocol, data passes only to the authorised users.

VI. CONCLUSION

In this paper, we have identified the security vulnerabilities in data discovery and dissemination when used in WSNs, which have not been addressed in previous research. Also, none of those 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 be easily intercepted. 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.

REFERENCES

[1] J. W. Hui and D. Culler "The dynamic behavior of a data dissemination protocol for network programming at scale", *Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst.*, pp.81 -94 2004.

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

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

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

[5] Daojing He, Sammy Chan, Shaohua Tang and Mohsen Guizani, "Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks", IEEE transactions on wireless communications, Vol. 12, No. 9, September 2013.

[6] P. Levis, N. Patel, D. Culler and S. Shenker, "Trickle: a self regulating algorithm for code maintenance and propagation in wireless sensor networks", in Proc. 2004 NSDI, pp. 15-28.

[7] G. Tolle and D. Culler, "Design of an application-cooperative management system for wireless sensor networks," in Proc. EWSN, pp. 121–132, 2005.

[8] Lin, K., Levis, P.: "Data discovery and dissemination with dip." In: Proceedings of the 2008 International Conference on Information Processing in Sensor Networks (IPSN 2008), Washington, DC, USA, IEEE Computer Society (2008) 433-444.

[9] T. Dang, N. Bulusu, W. Feng, and S. Park, "DHV: a code consistency maintenance protocol for multi-hop wireless sensor networks", in Proc. 2009 EWSN, pp. 327-342.

[10] Hui, J.W., Culler, D.: "The dynamic behaviour of a data dissemination protocol for network programming at scale." In: Proceedings of the 2nd international conference on Embedded networked sensor systems (Sensys 04), New York, NY, USA, ACM (2004) 81-94.

[11] Nildo dos Santos Ribeiro Junior, Marcos A. M. Vieira1, Luiz F. M. Vieira1 and Om Gnawali, "CodeDrip: Data Dissemination Protocol with Network Coding for Wireless Sensor Networks", In Proceedings of the 11th European conference on Wireless sensor networks (EWSN 2014), Feb. 2014.

[12] Hailun Tan, "Secure multi-hop network programming with multiple one-way key chains", In: Proceedings of the International conference on Embedded networked sensor systems (Sensys 07), Sydney, Australia, ACM.

[13] Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo, Li Xie, "Pollution Attack: A New Attack Against Localization in Wireless Sensor Networks", IEEE, WCNC-2009.

[14] I-Hong Hou, Yu-En Tsai, T.F. Abdelzaher, and I. Gupta. Adapcode: Adaptive network coding for code updates in wireless sensor networks. In INFOCOM 2008.The 27th Conference on Computer Communications. IEEE, pages 1517–1525, 2008.

[15] Andrew Hagedorn, David Starobinski, and Ari Trachtenberg. Rateless deluge: Over-the-air programming of wireless sensor networks using random linear codes. In Proceedings of the 7th international conference on Information processing in sensor networks, IPSN '08, pages 457–466, Washington, DC, USA, 2008. IEEE Computer Society.

[16] Daojing He, Member, IEEE, Sammy Chan, Member, IEEE, Mohsen Guizani, Fellow, IEEE, Haomiao Yang, Member, IEEE, and Boyang Zhou, "Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 4, APRIL 2015

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