Secure Distribution of Information Exchange in Various Channels using ARQ and Deterministic Network Coding

Manjusha.MS
University College of Engineering, Nagercoil

Banumathi.J
Assistant Professor, University College of Engineering, Nagercoil

Abstract –Wireless sensor network is a spatially distributed autonomous sensor, and to monitor physical or environmental conditions such as temperature, sound, pressure, etc. And spend together their data across the network to a main location. Eavesdroppers can use the valuable information during the data flows. So it is necessary to design network protocols that maintain secrecy of routes from eavesdroppers. To provide security, two secure transmission Schemes such as ARQ and Deterministic network coding are studied. ARQ is known as Automatic Repeat Request. It is an error control method for data transmission that uses acknowledgements and timer. DNC is known as Deterministic network coding. The DNC is used at intermediate nodes where the nodes take several packets and combine them together such that the eavesdropper cannot recover the value of the packets. The experiment results of these two secure transmission methods are show maximize in information flow and reduces the security cost for private channel. The future work is RLC. This is a Random Linear coding method which is used to code the packets for security purpose.

Index Terms – Public and Private Channels, Automatic Request Query or request (ARQ), Deterministic Network coding (DNC), Eavesdroppers.

1. INTRODUCTION

Wireless sensor network is a group of specialized transducers with a communication infrastructure that uses radio to monitor and record physical or environmental conditions. Wireless sensor networks (WSNs) [12] have gained world-wide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors. These sensors are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors. These sensor nodes can detect, measure, and gather information from the environment and on the basis of certain decision-making processes at the local level they can transmit the sensed data to the user.

Sensor nodes, is for performing some data and communicate with other nodes in the network. The sensor node has less memory and it cannot process large amount of information Wireless nodes, contains some components and its power is low compared to other networks. The sensor node memory is also limited and it performs many operations. Sensor node consists of a low power device and it also contains one or more sensors, memory, power supply, radio and actuator. In wireless networks, the data is send from the sender to the receiver using the two channels. First, the sender, send the data or information to the receiver in the presence of hackers, through the two channels are public channels and private channels. The public channel means, anyone can easily see or hack any messages during the data transmissions. But the private channels means, anyone cannot access the original messages during the data transmission.

The Wireless Sensor Network consists of no infrastructure and it also consists of several sensor nodes they are all working together to transmit the data together to prevent a region to obtain the information about other environment.

There are two types of WSNs:

- Structured
- Unstructured

A structured network is that fewer nodes can be deployed with lower network maintenance and management cost. Fewer nodes can be deployed now since nodes are placed at specific locations to provide coverage while ad hoc deployment can have uncovered regions. An unstructured WSN is one that contains a dense collection of sensor nodes. Sensor nodes may be deployed in an ad hoc manner into the field.

The remainder of the paper is organized as follows: Section 2 describes the related work. Section 3 describes the proposed work. The results of our comparative evaluation study are presented in Section 4. Section 5 concludes the paper.

2. RELATED WORK

The information exchange in various channels and also, with the risks of the security are to be considered in data transmission in [5]. It focuses mainly on how and why to establish the connection in both the private and public channels, and it also to prevent attacks from the secure channels. Encryption and decryption are takes place during the data transmission in [7,8]. In an organization they exchange their information between two systems. In a business level the information can be exchange either inside their organization or other users.

All the related works that have been done by other researchers that are related to the current research problem should be summarized in this section. Times New Roman font with size 10 must be used in this section. Sub topic should be written as given below:

- Communication complexity of secure distributed computation in the presence of noise
- Networking with secrecy constraints
- Disadvantages

2.1 Communication complexity of secure distributed computation in the presence of noise

The information is exchange over a noisy channel in [12] and it is a simple model for data transmission. An alternative protocol is used to exchange the bit between the two systems. First the public channel is considered along with the bit to be transmitted between the sender and the receiver and find the error in the data. Second, the case of the availability of an additional secret channel is considered.

Let x and y be finite sets, X and Y random variables uniformly distributed over x and y respectively. Let f be a function from x × y to {0, 1}.Processor P_x knows the value of X and P_y Knows the value of Y. P_x and P_y communicate according to a predetermined protocol, in order to exchange their values for the purpose of computing f .An eavesdropper, who knows both their protocol and the function f, listens to their communication in order to obtain information about f(X, Y).Processors P_x and P_y want to make sure that for every value(x, y) of (X, Y) the eavesdropper's probabilities of {f (X, Y) = 1} before and after the communication takes place, are ∈ -close.

The two processors use a deterministic protocol P. For every (x, y) ∈ x and y, P specifies the following sequence:

$$(1) \qquad < T_i, B_i , S_i >, \ i = 1,..., N,$$

Where,T_i describes the originator of the ith bit (P_x or P_y),B_i describes the bit itself (0 or 1),S_i denotes the channel used (secure or public), and N is the total number of bits communicated. An eavesdropper who knows the originator of each bit can decode only the publicly communicated bits constructs the modified sequence: $< T_i, B_i, S_i >, \ i = 1,..., N,$

Where

$$(2) \qquad B_i' = \begin{cases} B_i & \text{if } S_i = \text{public}, \\ 0 & \text{if } S_i = \text{secure}. \end{cases}$$

If S_i = secure, the eavesdropper will have to guess the value of B_i. A protocol is said to be $\in -$secure if for all transmission sequences e = < (T_i,B_i,S_i)>, The eavesdropper's a priori and a posterior probabilities of f(X,Y) = 1 are $\in -$close.

2.2 Networking with secrecy constraints

Providing security [20] is crucial to military wireless sensor network operation. The wireless medium makes networks vulnerable to a wide range of attacks by adversaries. Active attacks such as jamming or node replication are countered by using sophisticated intrusion detection mechanism. Where in eavesdroppers monitor transmissions from nodes.

Let a graph G = (V, E) that represents the wireless sensor network, where G represents the graph, V represents the set of nodes and E represents the set of links in between the set of nodes. Let (A, B), is a node in the graph and E represents that the node B listen the node A for data transmission. Then, consider the value Y= { Ya(1), Yb(2),….} and it denotes the time at which the packets are transmitted by the node A.

$$(3) \qquad T_A = \lim_{n \to \infty} \frac{n}{Y_A}$$

Where, TA represents the rate of the transmission of a node A and it is defined as the average number of packets are to be transmitted by the node A.

The node, share a secure channel during the data transmission in a wireless network with the presence of the eavesdroppers. If the channel is not secure means problem will occur such as fading, data and path loss and interference. Let A= {A_1, A_2 ,…, A_k} denotes a group of nodes and T= {T_{A1},T_{A2},…T_{Ak}}

denotes the transmission vectors. The set of transmission vectors $\{T_{A1},T_{A2},..T_{Ak}\}$ be denoted by C (A).

2.3 Disadvantages

- No security consideration.
- The costs in the private channel are higher.
- Problem of information exchange under secrecy requirements in wireless systems.
- Minimum number of bits should be transmitted over the private channel.

3. PORPOSED MODELLING

Consider the problem of exchanging the information between the sender and the receiver through various channels in the presence of eavesdroppers. Thus, the important one is that, to use the private channels for data transmission. Due to this private channel the cost and delay are to be decreased. The overall problem combines the issues of communication complexity, security, and energy/delay performance cost. Our approach does not consider information theoretic security but, rather, communication complexity, consider the problem of streaming a file by exchanging information over wireless channels in the presence of an eavesdropper.

The overall problem combines the issues of communication complexity, security, and energy/delay performance cost. Our approach does not consider information theoretic security but, rather, communication complexity, consider the problem of streaming a file by exchanging information over wireless channels in the presence of an eavesdropper. Two channels are used for data transmission they are the public and the private channel and use the single and multiple users for data transmission. Two methods are used here simple Automatic Repeat Request (ARQ) and Deterministic Network Coding (DNC) for data transmission.

- Data transmission in channels
- ARQ
- Deterministic network coding
- Advantages
- Proposed Architecture

3.1 Data transmission in channels

Let P private, D be the probability of successful packet reception by destination D and let P public, D and p denotes the packet is received by the receiver successfully in the presence of the hackers. It is required that the source deliver the file to the destination while keeping it secret from the eavesdropper. It is required that the source deliver the file to the destination while keeping it secret from the eavesdropper. The hacker received the packets through the wireless channels. Those received packets are less than the target value. To transmit the packet reliably we assume that the source can use either one of two methods of transmission:

• Simple Automatic Repeat Request (ARQ)

• Deterministic Network Coding (DNC)

In each time slot, the source forms M linearly independent deterministic combinations of the M packets and then uses simple ARQ to transmit each linear combination reliably to the destination, assume in this case that the receiver does not make inference from the received linear combinations but either decodes the transmitted packets or not. Instant error-free acknowledgements are assumed in all cases as is usually assumed in similar investigations. The objective is to find the minimum number of packets that the source should transmit through the private channel in order to minimize an appropriate cost subject to the secrecy requirement. Two types of costs are considered respectively: the extra energy spent and the extra delay required, transmit through the private channel. In what follows, the problem is explained in detail for both cases when simple ARQ and Deterministic Network Coding (DNC) are used respectively.

3.2 ARQ

The simplest way of error detection and checking is the ARQ. ARQ stands for Automatic Repeat Request, the below figure shows the operation of ARQ. First, the sender, encode the packets and send it to the receiver through the communication channels. The ARQ involved in that, and checking if any errors occur in the messages during data transmission. If any error, occur means it send NACK to the feedback channel. The source sends the same message to the receiver. If no error occurs means the receiver, send the Acknowledgement (ACK)

to the sender through the feedback channel.

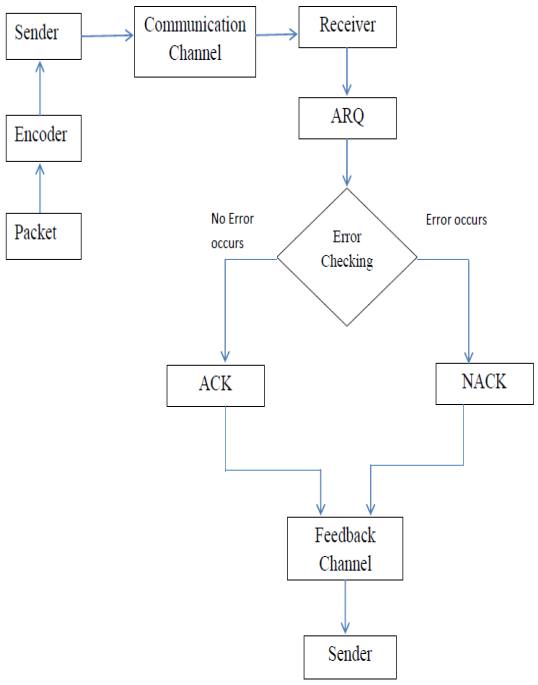

Fig: 1 Automatic Repeat Query

3.3 Deterministic network coding

Deterministic Network Coding (DNC), where in each time slot, the source forms M linearly independent deterministic combinations of the M packets and then uses simple ARQ to transmit each linear combination reliably to the destination. We assume in this case that the receiver does not make inference from the received linear combinations but either decodes the transmitted packets or not.

In this case, the source S constructs a system of M linearly independent combinations of the M packets such that the eavesdropper cannot recover the value of any of the M packets except if it receives successfully all M linearly coded packets. The conditions under which a linear system of equations satisfies the above property are presented, and a method is provided to construct a linear system satisfying this property.

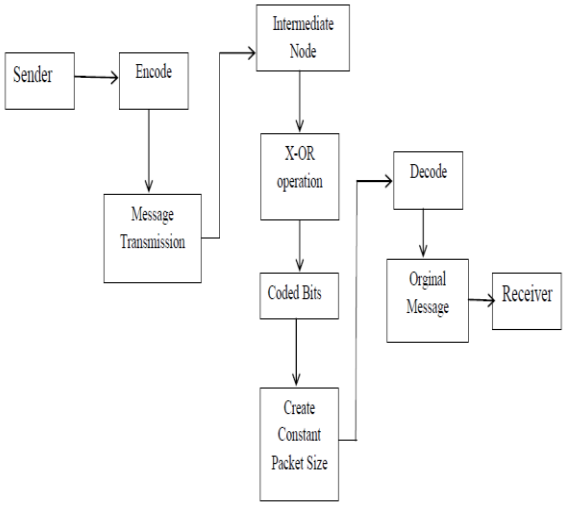

Fig: 2 Deterministic Network Coding

3.4 Advantages

- Secure Data Transmission.
- Network Coding considerably reduces the security cost.
- Low complexity.
- ARQ reduces the delay of transmission.
- Low Computation Overhead.

3.5 Proposed Architecture

The administrator acts as a user and it stores large amounts of data or files in their database.User1 acts as a source and it sends one request for registration to the administrator. The administrator issue the certificate for registration to the user1 (source).

After getting the certificate for registration from the administrator then only the user1 register all the details that includes (name, password, first name, gender, user type, date of birth, port number, address, city, state, cell no, email id). Information is stored in the SQL database. Generate the public and private key for data transmission. Then login in to transmit the files from sender to the receiver. For login in to the form enter the name of the user and public key. If correctly entered the details then the authorized person only

login in to transmit the data from the sender to the receiver through the private channels in the presence of eavesdroppers.

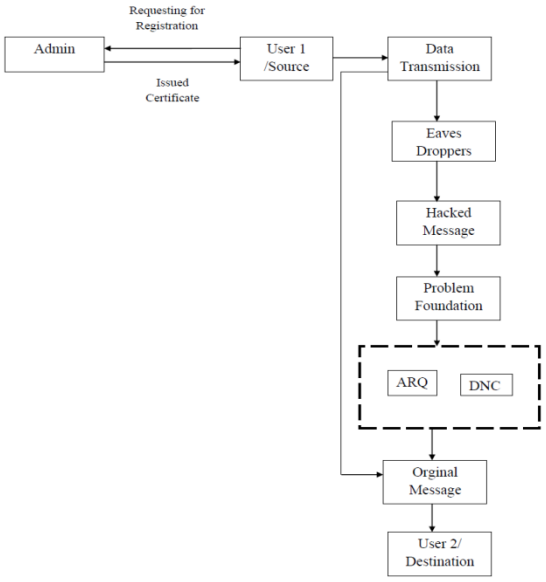

Fig: 3Proposed Architecture

Eavesdropper is a person that acts as a third party. If we transmit the files from the sender to the receiver in the presence of eavesdropper it may have the chance to hack the files. Eavesdropper then changes the contents or doing some modifications in the files send from the sender to the receiver. Some problems will occur.

ARQ is to detect any attacks involved in that and then show it to the user. DNC is used to shows the attacked files and with the original files. Clear that problems and send the original message to the destination. Otherwise it sends original files directly to the destination.

After overcome the problems found in transmitting the files from the sender to the receiver. Finally the original file is received by the user2 (destination) from the user1 (source).

4. Performance Metrics

The performance metrics are to be calculated here is the Signal to Noise ratio, Error detection, cost and delay. Cost in the private channel and delay are to be reduced. Error detection is to be increased. In [7] it mainly focuses on the metrics like throughput and delay. The other performance metric such as the energy and delay are calculated in [8]. In other references many other performance metrics are calculated.

- Network Delay
- Packet Transfer Delay
- Performance Analysis

4.1 Network Delay

Network delay may happen during the exchange of data between the sender and the receiver. Due to traffic in network, delay may occur. Delay means how long it takes time to send the message to the receiver or when the receiver gets those information from the sender [3,5]. The sender takes the delay of the network and find where the delay our [1,4]. Both the maximum and average delay, and they divide the delay into several parts:

- Processing delay - time routers take to process the packet header
- Queuing delay - time the packet spends in routing queues
- Transmission delay - time it takes to push the packet's bits onto the link
- Propagation delay - time for a signal to reach its destination.
- Queuing delay - time the packet spends in routing queues
- Transmission delay - time it takes to push the packet's bits onto the link
- Propagation delay - time for a signal to reach its destination.

4.2 Packet Transfer Delay

Packet transfer delay is also a performance metrics. The sender send the data or information to the receiver, it first split the data in to some packet size it may depend on the user. Due to, the transmission of channels or any hackers involved in that it takes some delay to reach the receiver. Sometimes the packet may be loss due to any traffic in the channels over the wireless networks. There are four sources of packet transfer delay:

- Nodal processing:

- Check bit errors
- Determine output link
- Queuing.

The file is distributed among multiple nodes, where the nodes are required to exchange their portions of the file until all nodes possess the entire file [2, 13]. Nodes can choose to transmit through public channels to which an eavesdropper may have direct access or through private secure channels that are not accessible to the eavesdropper [13]. Direct access or through private secure channels that are not accessible to the eavesdropper [13]. Random Network Coding was used. But, the network costs and other system parameters were just defined as constants.

4.3 Performance Analysis

The performance evaluation for the security cost also the optimal number of nodes are to be used as represented in the below figures.we compare the performance of the secure transmission using arq to the case when deterministic network coding(dnc) is used. Also,we investigate the effect of the security level parameters n and lambda on the minimum security cost.

The following values for the system paramaters are used, p=2watts, m=7, n_0=0db, $p_{private,d}$=0.368, $p_{public,d}$=0.0606, pe=0.535. The minimum delay for the case when the value of the security level parameter n is varied between 0 and 7. Two values of lambda=0.0,0.5.the minimum security cost and the optimal number of packets that should not be transmitted through the public channel.

4.3.1 Security cost as a function of security parameter

The security cost as a function of the security parameter n is as shown in the below figure. It shows that as the security transmits through the public channel inreasaes and hene the security cost decreases. Also for any value of the security level parameters n and lambda,the security cost,when using Network coding, is considerably lower than when using ARQ. This is because due to the structure of the network coded packets, the receiver can not decode any of the packets unless it receives sucessfully the M coded pakets.

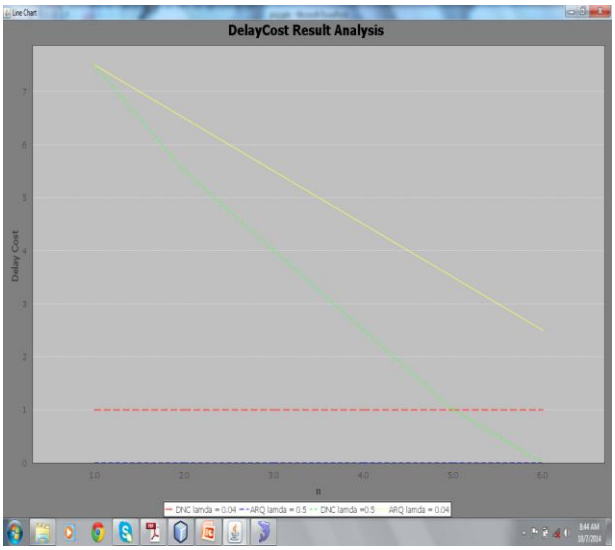

Fig: 4 Security cost as a function of security parameter n

Hence the probability that the eavesdropper decodes sucessfully n or more packets when the source transmits all of the M coded packets is considerably lower than the case of ARQ.

Also for any security level parameter n, the transmitter can at most send one packet over the private channel when using DNC and even send no packets through the private channel when the value of the lambda is high,which results in considerable seurity costs savings when using DNC compared to ARQ.The delay cost is represented as in axis and the number of packets n is represented in y axis.The red dotted line represents the DNC and the lambda value is equal to 0.04 and Green line represents the the ARQ and the value of lambda is equal to 0.5 and the yellow line represents again ARQ and the value is 0.04.

4.3.2 Optimal nodes as a function of security parameter n

We consider that the nodes have the same private channels quality among each other. We define $P_{private}$ channel between each pair of nodes. Also for the values we consider 7 nodes in the network where each node has 3 packets. As for the system parameters we consider the following values for the probabilities of success: PE=0.535, Ppublic=0.99, Pprivate =0.606. For both the ARQ and DNC, the optimal number of the nodes that should transmit through the public channel and the minimum delay cost are computed for the case when the security parameter n is varied between 1 and 10 packets. Two packets of lambda are onsidered respectively:

lambda=0.04,0.8. And it shows that for both cases of ARQ and Network Coding he optimal number of pakets that transmit through the public channel increases as the security parameter n increases.The optimal number of nodes that transmit through the public channel increases as the security parameter n increases.Also for both cases, the onsidered values of lambda, the optimal number of nodes is higher for the case of Network Coding than the case of ARQ.

This is because in the case of NC, the eavesdropper should decode all the packets transmitted by each node. This consequently decreases the probability that the eavesdropper receives the target number of packets, and hence for high values of lambda, all the nodes can transmit using Network Coding through the public channel.

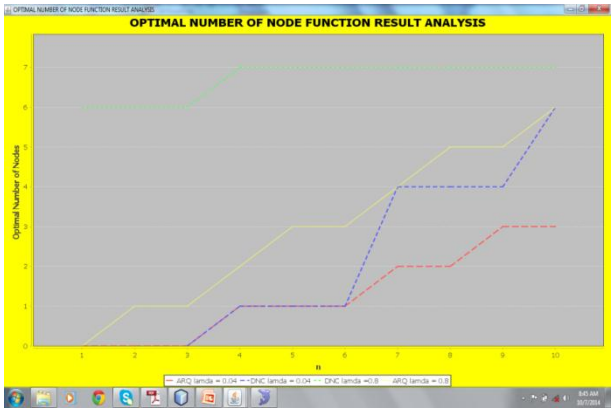

Fig: 4.2 Optimal nodes as a function of security parameter n.

Two reasons are to be considered. First one is the number of nodes that should transmit through the public channel is higher for the case of Network Coding than ARQ. The second reason is that each node needs to transmit only one packet through the private channel in the case of Network Coding while in the case of ARQ each node has to transmit all its packets through the private channel.Yellow and green line represents the ARQ and its value is lambda=0.04,0.8. Red line represents the DNC and its value is lambda=0.04.

Value 1	Value 2	Value 3
3	3	2
5	6	4
7	8	9

Fig: 1 Table for the proposed system

4.3.3 Proposed System Graph

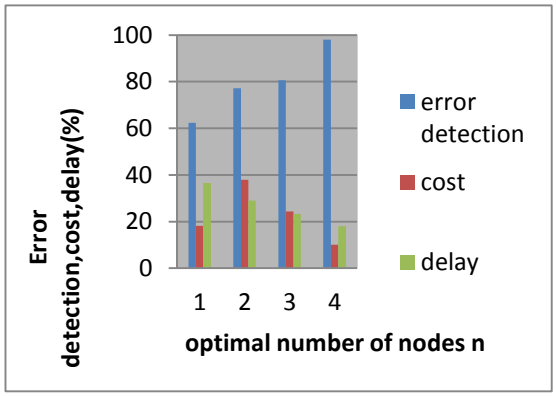

Fig:5 Proposed system graph for Security Parameter

The proposed system graph denotes the value of error detection, cost and delay. X axis represents the optimal number of nodes n and y axis represents the security parameters such as the error detection, cost and delay. In this proposed paper, the error detection is 98%, cost is reduced to 10.6 and delay is reduced to 18% .So the proposed system is better compared to the existing system.

4.3.4 Existing system graph

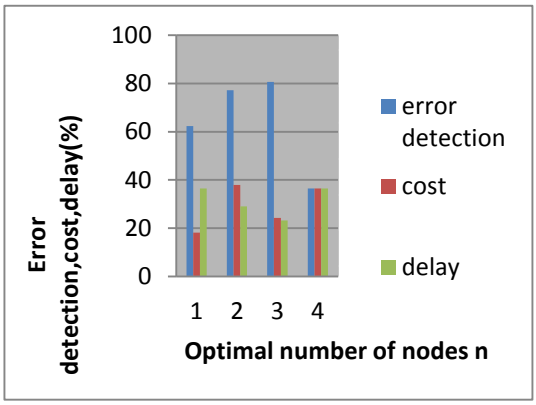

Fig:6 Existing system graph for security parameters

5. Conclusion

In this project, I have experimented secrecy of routes by using two transmission schemes such as Automatic Repeat Query (ARQ) and Deterministic network coding (DNC).The issue of secure transmissions in a wireless fading network in which a file is required to be delivered while keeping it secure from an

eavesdropper. So, we use two transmission schemes ARQ and DNC. The results show the tradeoff between achieving a certain level and the cost incurred. Also it reduces the security cost compared to the case when simple ARQ is used.

REFERENCES

[1] Ahlswede. R, Cai. N, Li S.Y, and Yeung .R, "Network information flow," IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[2] Bhattad .K and Nayayanan .K, "Weakly secure network coding," in Proc. Workshop Netw. Coding, Theory Appl., Riva del Garda, Italy, Apr. 2005, pp. 1–6.

[3] Blom R (1982) "Non-public key distribution. In: Advances in cryptology"—CRYPTO 82, pp 231–236

[4] Blundo .C, De SantisA, Herzberg .A, Kutten .S, Vaccaro .U and Yung.M, "Perfectly Secure Key Distribution for Dynamic Conferences", (1992) pp. 471–486

[5] Bulusu V, Durresi A, Paruchuri V, Durresi M, Jain R (2006) "Key distribution in mobile heterogeneous sensor networks". In: Global telecommunications conference, 2006. GLOBECOM '06. IEEE, New York, pp 1–5. ISBN 1-4244-0356-1.

[6] Cai.N and Yeung R.W, "A security condition for multi-source linear network coding," in Proc. IEEE ISIT, Nice, France, Jun. 2007, pp. 561–565.

[7] Cai .N and Yeung .R, "Secure network coding," in Proc. IEEE ISIT, Jun. 2002, pp. 323–329.

[8] Camtepe S.A and Yener .B, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", Networking, IEEE/ACM Trans. on, vol. 15, no. 2, (2007) April, pp. 346-358.

[9] Chan H. , Perrig A. and Song D. , "Random key pre-distribution schemes for sensor networks", Proc. IEEE Symp on Research security privacy, (2003) May 11-14, pp. 197- 213.

[10] Chan H, Perrig A (2005) "Pike: peer intermediaries for key establishment in sensor networks". In: INFOCOM 2005. 24th annual joint conference of the IEEE computer and communications societies, pp 524–535. ISBN 0-7803-8968-9

[11] Cheikhrouhou Y. -H. , Koubaa A. , Boujelben M. and Abid .M, "A lightweight user authentication scheme for Wireless Sensor Networks", 2010 IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), (2010) May 16-19, pp. 1-7.

[12] Chuang I.H, Su W.-T, Wu C.-Y, Hsu J. -P. and Kuo Y. -H. , "Two-Layered Dynamic Key Management in Mobile and Long-Lived Cluster-Based Wireless Sensor Networks", Wireless Communications and Networking Conference, WCNC 2007, IEEE, (2007) March 11-15, pp. 4145-4150.

[13] Du .W, Deng .J, Han Y. S., Chen S. and Varshney Pr. K., "A Key Management Scheme for Wireless Sensor Network Using Deployment Knowledge", IEEE INFOCOM, (2004).

[14] Eschenauer .L and Gligor V.D, "A key management scheme for distributed sensor networks", Proc. of the 9th ACM Conference on Computer and Communication Security, (2002) November, pp. 41-47.

[15] Feldman .J, Malkin .T, Servedio .R, and Stein .C, "On the capacity of secure network coding," in Proc. Allerton Conf. Commun., Control, Comput., Sep. 2004, pp. 1–10.

[16] Gay D, Levis P, von Behren R, Welsh M, Brewer E, Culler D (2003) The nesc language: a holistic approach to networked embedded systems. SIGPLAN Not 38(5):1–11. ISSN 0362-1340. doi:http://doi.acm.org/10.1145/780822.781133 16.

[17] Girod L, Stathopoulos T, Ramanathan N, Elson J, Estrin D, Osterweil E, Schoellhammer T (2004) A system for simulation, emulation, and deployment of heterogeneous sensor networks. In: 2nd inter- national conference on embedded networked sensor systems, 2004 17.

[18] Girod .L, Stathopoulos .T, Ramanathan .N, et al., "A System for Simulation, Emulation, and Deployment of Heterogeneous Sensor Networks", Proc. of ACM SenSys, (2004).

[19] Han .K, Ho .T, Koetter .R, Medard .M, and Zhao .F, "On network coding for security," in Proc. IEEE Military Commun. Conf., Orlando, FL, USA, Oct. 2007, pp. 1–6.

[20] Heinzelman W. R. , Chandrakasan A. and Balakrishnan .H, "An application-specific protocol architecture for wireless micro sensor networks", IEEE Transactions on Wireless Communications, vol. 1, no. 4, (2002), pp. 660-670.