MULTICAST DATA COMMUNICATION IN WSN USING DIFFIE-HELLMAN ALGORITHM FOR SECURE DATA TRANSFER

Ms.C.Suganya, M.Phil Scholar,

PG & Research Department of Computer Science,

Chikkanna Govt. Arts College, Tirupur.

Dr.K.Nandhini, Assistant Professor,

Department of Computer Science,

Chikkanna Govt.Arts College, Tirupur.

Abstract: A Wireless Sensor Network (WSN) contains large number of Sensor nodes. These sensors have the ability to communicate among each other. To exchanging the information, network should give higher correspondence strategy among WSN and will give detecting the node between the networks. In WSN, detecting the node might be a pivotal issue to exchange the information among the nodes while communicating it faces the security issues. Privacy of the user may loss because of unauthorized access of third party. For this issue this paper proposes a Diffie-Hellman Algorithm of public key encryption method to provide more security to the data also here included the multicast method of communication with dynamic node discovery technique to solve the security issues.

***Keywords**: Wireless Sensor Network, Security, Sending Message and Multicast Communication.*

I.INTRODUCTION

A Wireless Sensor Network (WSN) contains huge amounts of Sensor nodes. Through the base-station (BS), the sensors nodes were communicating each other in a network. A bigger assortment of sensors licenses for detecting over bigger countries with bigger exactness. Wireless Sensor Networks provide a lot of Sensor nodes that outline the networks for recognition the unfurl of technique and advance learning with respect to the objectives of result back to the end-clients. To exchanging the information, network should give higher correspondence strategy among WSN and will give detecting the node between the networks. In WSN, detecting the node might be a pivotal issue to exchange the information among the nodes [1]. While detecting the node inclusion might be a noteworthy drawback on account of disappointment, power, or commotion precariousness. The significance of this difficulty emerges once a WSN must be set up in inaccessible and commonly unclean space. In those regions, there are a few sections like temperature that must be recorded extremely precisely to evade a blast [2]. Each explosion will build the contamination inside the atmosphere that may be more regrettable in an exceedingly blustery climate. In such zones, a sensor is expected to be sent all over. In any case, there's no assurance that the nodes a consistently disseminated when irregular preparing. the possibility of covering the detecting field while they're not covered and being inside correspondence differ of each choice to be completely associated are diminished [3]. Moreover, keeping up enclosure is significant of Sensor nodes was in decreasing of the battery channel. Wireless network is one of the critical viewpoints for the clients while they traverse the networks. With the upgrade of versatile innovations individuals are as often as possible requires privacy and security in communicating networks. Security and privacy protecting are significant one to exchange the information through network. Communication in WSNs more often than not happens in specially appointed way, and shows similarities to wireless unplanned networks. Similarly, WSNs are dynamic as in radio range and network availability changes by time [4]. A sensor node kicks the bucket and new sensor nodes might be added to the network. In a WSN, multicast is a more productive strategy for supporting gathering communication than unicast, which can spare data transfer capacity and vitality to a great extent. Since sensor nodes experience the ill effects of restricted assets, for example, low algorithm ability, little memory, constrained vitality assets and low data transfer capacity, multicast is broadly utilized in sensor-based applications, for example, condition checking, human services observing, and so forth. When all is said in done, multicast is unquestionably more defenseless than unicast on the grounds that the transmission happens over multiple network channels. It is a significant issue to guarantee the security for the multicast correspondence in WSNs. Because of the asset requirements of sensor nodes, security in WSNs forces a few difficulties which are more unpredictable than those in the other normal networks[5]. In the meantime, the vast number of sensor nodes utilized to screen basic parameters, the absence of a particular network engineering or foundation, and the regular topology changes because of the nodes versatility likewise bring the difficulties when we structure the gathering key administration convention. A sensor network is a unique sort of network. It imparts a few shared characteristics to run the PC network, yet in addition presents requirement. In this manner, we can think about the prerequisites of a wireless sensor network as including both the regular network necessities and the interesting necessities fit exclusively to wireless sensor networks[6]. We can group the security objectives into two objectives: primary and optional. The fundamental objectives incorporate security destinations that ought to be accessible in any framework (classification, accessibility, respectability and validation). The other classification incorporates auxiliary objectives (self-association, secure limitation, Time synchronization and Resilience to assaults). The Domain of multicast networking and security related issues is a wide specialized subject. Inside the problems permitted, we examine couple of applicable specialized issues and execution transactions to see while applying security and key administration methods in help of multicast networking [7]. First, we think about the use of existing and proposed security methods for multicast networking, including key dissemination, dynamic key administration, and unwavering quality issues. All through in the paper we provide security strategy using Diffie-Hellman Algorithm in Multicast networks. The Diffie-Hellman key Exchange convention is a cryptographic convention that was created by Whitfield Diffie and Martin Hellman in 1976. The Diffie-Hellman key Exchange algorithm is the accompanying difficulty. Alice and Bob need to share a mystery key for use in a symmetric figure, however their solitary methods for correspondence is uncertain.

II. LITERATURE REVIEW

SwapnaNaik [6] detected data can be sent from various perspectives, before unicast steering was there to a solitary sink node, but because of the wide assortment of WSN applications the nearness of multiple sinks is acknowledged which requires multicast directing for effective information scattering to multiple goals. For any catastrophe reconnaissance or flame dealing with crisis situations different multicast directing protocols have been proposed by numerous analysts. This paper provides an overview of the current multicast directing protocols by exhibiting approach, their preferences and burdens. Further a near investigation of different multicast protocols is done based on various parameters to recognize various issues and moves that should be settled for every last one of them.

P.PrasannLaxmi [7] WSNs discover applications in zones like human services, home robotization, traffic control and so forth. WSN with qualities of self-association, multi-hop, dynamic topology and constrained vitality assets, make it amazingly hard to draw out the lifetime of the network. To drag out the existence time of WSN with restricted vitality assets, Multicast can all the more likely meet the prerequisites of network assets. It has a functioning importance for WSN to expand its execution sooner rather than later. And proposed methodology contrasts the execution of two protocols and ten nodes in each gathering. Creator break down the proposed answer for assess the execution utilizing Network Simulator-2 (NS-2) under various network parameters with various goal nodes.

L. B. Jivanadham [8] propose an efficient group key management utilizing symmetric key and Threshold Cryptography for Cluster based Wireless Sensor Networks. The proposed plan considers a progressive bunch structure of sensor network and embraces the pair-wise key administration and gathering key administration dependent on limit key cryptography to create and to disseminate the keys effectively inside a group and updates occasionally keys. By thusly EGKMST gives ceaseless transmission security and dodges perilous assaults from noxious nodes and moderate the node bargain assault in WSNs correspondence. The security and execution investigation delineate that EGKMST conspire accomplishes the necessity of gathering correspondence and gives productive security low correspondence cost, low memory overhead and vitality sparing contrasted and some current key administration plans.

Fan, Yanfei, et al [9]. Consider the privacy threat in multihop wireless networks, with this threat where assaults, for example, traffic examination and stream following can be basically occurred by a malevolent challenger because of the Public atmosphere of the wireless medium. For this network coding has the inactive one to anticipate these assaults since the coding/blending process is certain at middle of the road nodes. Be that as it may, with the straightforward misuse of network coding can't finish the objective once adequate bundles are made by the challenger. In other manner, with the assistance of existing privacy-safeguarding strategies of onion steering, the coding/blending nature counteracts the likelihood of abusing. For this the creators propose network coding-based privacy-safeguarding technique alongside the traffic examination in multihop wireless networks. They use the hemimorphic encryption component on the Global Encoding Vectors (GEVs), their plan gives two noteworthy privacy-protecting highlights, bundle stream un-recognizability and message content classification, for ably anticipating the traffic examination assaults.

Xiaojiang Du, [10] have proposed a safe and successful key administration plot dependent on powerfully bunching of WSN. Their convention embraces the primary thought of limit mystery sharing plan, joins the qualities of dynamic key administration plan and updates key data intermittently. This coordinated strategy not just gives solid security and obstruction of caught assault, yet in addition fulfills the needs of the versatility. Creator has proposed a vitality proficient half and half key administration (EHKM) convention. Their procedure has considered the heterogeneous security necessities of a wireless sensor networks. In this way, they have achieved varying dimensions of security with least correspondence overhead.

III. METHODOLOGY

The application of wireless sensor networks to areas such as combat field surveillance, terrorist tracking and highway traffic monitoring requires secure communication among the sensor nodes, which under this collaborative model calls for efficient group key management. However, providing key management services in wireless sensor networks is complicated by their ad-hoc nature, intermittent connectivity, large scale, and resource limitations. To address these issues, this paper proposes a new energy-efficient key management scheme for networks based on secret sharing, in which the secret shares are calculated by the cluster heads which choose the one-order polynomial to improve efficiency, the symmetric keys preloaded into the nodes are used to encrypted secret shares to insure security [11]. We analyzed the security and performance of this scheme compared with other ones. Comparison results show that our scheme is low in storage requirement, computational overhead and communication cost.

- These are very critical in multicast communication. In small scale sensor network, it is easier to capture the data, process it, and forward to sink.
- But in random and dynamic network of large size, it usually doesn't go by single hop communication.
- The nodes are formulated in groups, where each group member interacts with other group member to forward the processed data from one point to another.
- The process of data aggregation completely fails without multicast communication. Hence, it is very important that a robust security technique is to be developed to address the security issues in group communication system in WSN.

Wireless sensor networks WSNs effectively tolerate different attacks due to its defenseless condition, restricted plan of action and open correspondence channel. Validation is one of the extremely viable approaches to prevent unapproved and defiled interchanges from being sent in wireless sensor networks (WSNs). Along these lines, many message verification plans have been created, in light of either symmetric-key cryptosystems or open key cryptosystems. A considerable lot of them, yet, have the impediments of high computational and correspondence cost however absence of adaptability and solidarity to node bargain issues. To address these issues, creator proposes Diffie-Hellman key Exchange convention. Along these lines, the security of the key appropriation and the board in wireless sensor networks will get comprehended by this technique.

a. Attack Model and Secret Sharing Scheme

The attackers may originate from inside or outside the network. They can listen silently on the traffic infuse new messages, replay and change old messages, or different personalities. As of now referenced above, creator expect the TTP as totally dependable and the NMM as genuine however inquisitive. Creator further accepts that the Network Multicast Manager (NMM) does not work together with malicious nodes. Also, creator expect that the security related data at the nodes and at the NMM is put away in alter safe equipment, which is as of now normal and accessible at a sensible cost. Creator don't examine the systems to distinguish misbehavior of a node (e.g., by putting away trust tables in every node) and creator allude to the writing on interruption location components and confirmation instruments to identify anomalous conduct of a bargained node.

b. Key Distribution Phase

In the primary stage, the key dispersion stage, the TTP chooses three master secret values x, y, z F1qand produces two unique sorts of security related data. The first type is for the node's N_i with i = 1. . . m in the network and the second type is for the NMM. Denote the identity of Ni by IDi and NMM by ID_{NMM}.

For each N_i, the TTP executes the following computations:

$Ki = H (IDi \| x \| y\| z)$

$Ai = H (IDi \| x)$

$Bi = H(y) \oplus Ai$

$H(Ai) = H (H (IDi \| x))$

The qualities Ki, Bi, H(Ai), H(x), IDNMM are sent over a safe channel (for example by pre-stockpiling) to every node Ni. Here, Bi replaces the character of the node for the outside world. The parameter H(Ai) is utilized to validate its character with the NMM, and H(x) for the verification of the NMM with the node.

c. Node discovery

Creator accepts that the nodes have locally exceptional identifiers, i.e., no two neighbours of a given node have a similar identifier. For instance, the identifier could be the MAC address of a node or its area.

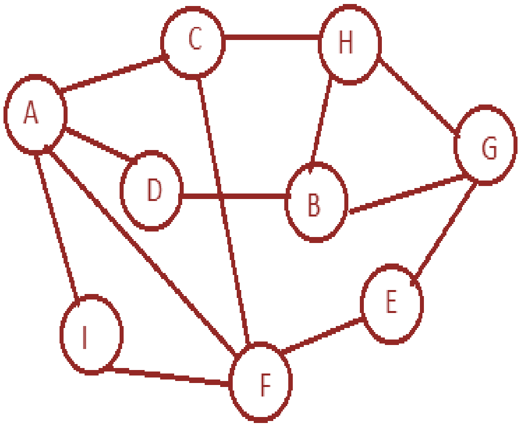

Figure 3.1: Node in WSN

In figure 3.1 all nodes were associated. From this creator need to discover the node which on will give a traffic free and speedy way to convey the bundle to the next node. The node which is halfway to source node will get the RREQ and sets up a turnaround way. This is finished by making the past hop of the solicitation message as the following hop on the switch way. Multiple quantities of RREQ messages came to at a similar node will be disposed of. This will essentially lessen the network burden and postponement in the network. As the RREQ message achieves the goal, a Route Reply (RREP) message is produced and sends back to the source node through a similar way pursued by the RREQ message. The following session is the Route Maintenance. At whatever point the association between any two nodes is harmed or lost, a Route Error (RERR) message is created and sends to all sources through forerunner courses which are kept up discretely. Pre-characterized courses are eradicated by RERR messages in like manner. At the point when a source gets a RERR message, it starts Route Discovery session once more.

d. Multicast Construction Phase

In view of the data got after the enlistment stage, the multicast bunches are made. For each gathering, a multicast address IDG is produced. The NMM communicates the location IDG to every supporter, signified by Ss, s = 1, . . ., n (with relating key material As, Bs). To the distributer of the gathering, indicated by P (with comparing key material Ap, Bp), key related data of the supporters in its gathering is sent utilizing their regular shared key kp. This key related data for every supporter equivalent to kps = H(IDGkks) and is joined with personality Bs, for all Ss with s = 1, . . ., n in the multicast gathering. Therefore, the message Ekp (B1, kp1... Bn, kpn) is sent to the distributer. After decoding of this message, P has a typical imparted key to every one of its endorsers. This data enables P to share a haphazardly picked gathering key kg for the multicast correspondence. Here, P initially picks an arbitrary esteem kg, which will fill in as the gathering key to be imparted to different individuals in a multicast correspondence message. It additionally chooses an arbitrary esteem h0 for the development of a single direction key chain to be utilized for verification purposes.

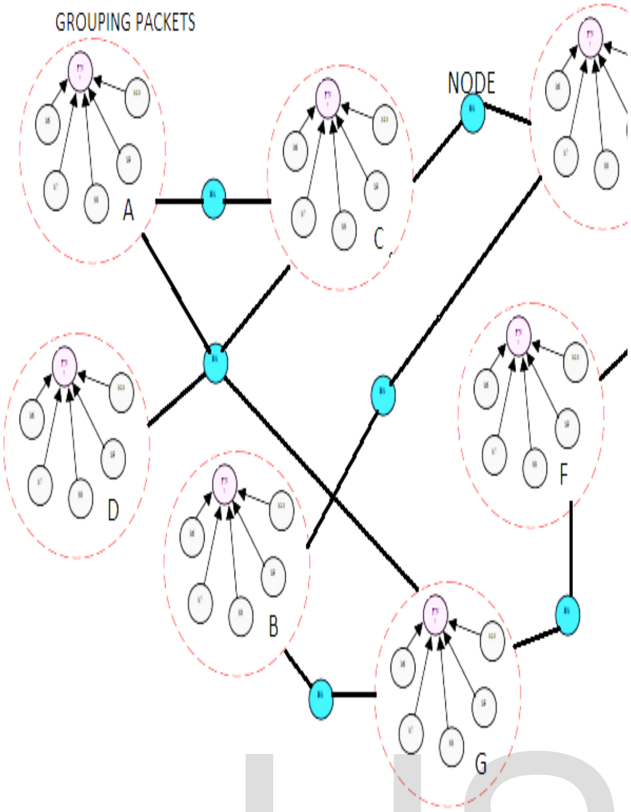

Figure 3.2: Proposed Architecture

Utilizing LI through the n focuses (xs, ys) = (Bs, kps) with s = 1, . . ., n, together with the point containing the gathering key (0, kg), a polynomial of degree n can be developed. Next, n different focuses (v, Vv) with v = 1, . . ., n on this polynomial are inferred. Diffie-Hellman builds up a mutual top mystery that can be utilized for mystery correspondences while trading information on the network. Diffie-Hellman key Exchange is a particular technique for trading cryptographic keys. It is one of the most punctual functional instances of key Exchange actualized inside the field of cryptography. The Diffie– Hellman key Exchange strategy permits two gatherings that have no earlier information of one another to together set up a mutual mystery key over a shaky correspondences channel. The Diffie-Hellman algorithm works flawlessly to create cryptographic keys which are utilized to encode the information being communicated over an open channel.

IV.RESULTS AND DISCUSSION

For system analysis, we have authorized the key management rule in NS2. Calculation costs are estimated as far as assortment of encryptions expected to change the keys inside the occasion of hub bargain and hub expansion. When a hub is another, exclusively the new irregular assortment and new id of the polynomial perform will be transmitted by base station. Singular hubs can get it and send it to the closest hub and it forward to the goal hub.

We provide the execution time to the majority of our conventions (if you don't mind note that the execution time for the science algorithms are frequently). We conjointly blessing the outcomes while not the execution time of the sink, since in a few applications, the base station might be a unique hub with extra assets. All outcomes are the midpoints of one hundred trials of each convention. We conjointly offer the quality deviations for execution time just as the season of S. We see that these qualities are little contrasted with the execution time of the convention.

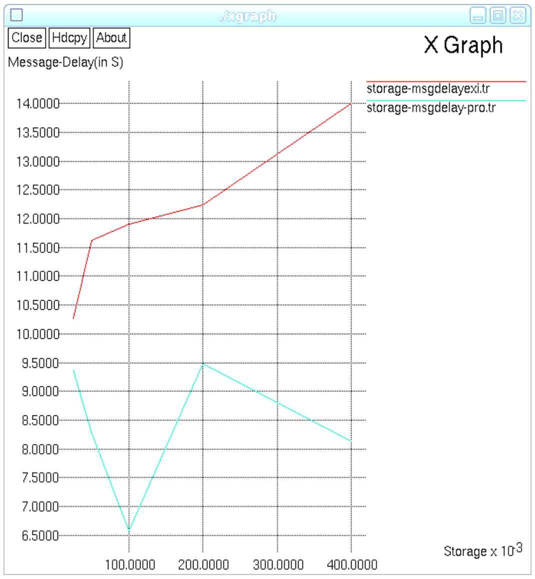

Figure 4.1: Message delay

In figure 4.1 it shows the performance comparison of delay of message was provided.

From this analysis delay of message was reduced in proposed technique for the quick receiving of the message.

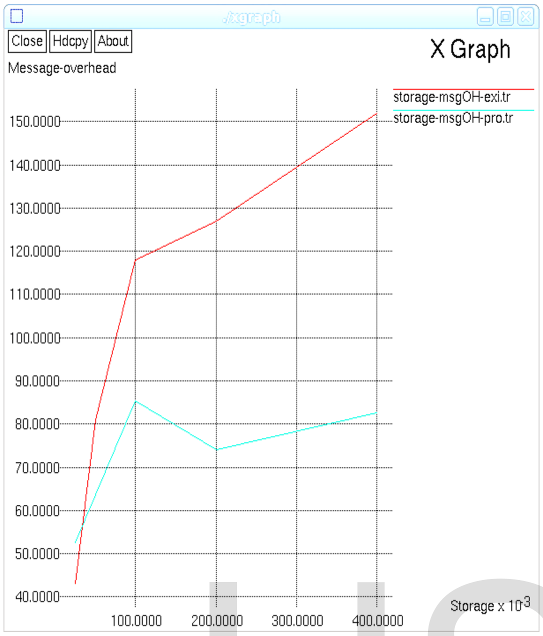

Figure 4.2: Message Overhead

In figure 4.2 messages overhead denotes to time and bandwidth. When compared to the existing one our system reduces the bandwidth and time for the message sending in network.

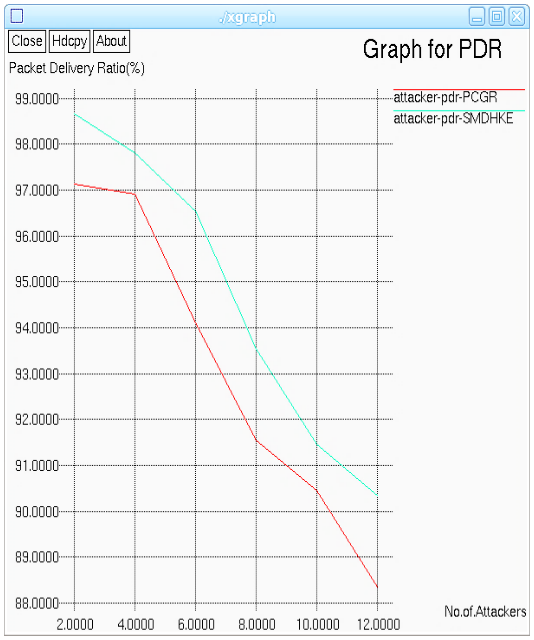

Figure 4.3: Packet deliver ratio

In this figure 4.3 it shows the deliver ratio of packets. Our system shows large number of packets was sent without packet loss.

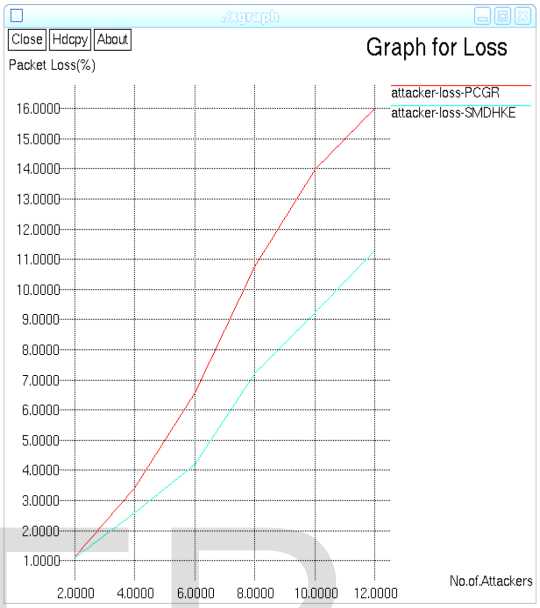

Figure 4.4: Packet loss

Packet loss is one of the great issues in network. In figure 4.4 shows the low-level packet loss. When compared to existing the packet loss was reduced.

V. CONCLUSION

The data that flows in among the sensor nodes in WSN consists of physically captured data from the readings of sensors, a mobile code, security using key management techniques, and location information of the sensor nodes. Owing to the lesser amount of obtainable of computational origin in the miniature sensor nodes and wireless communication social, WSN endures from probable security threat aspects. Security is one of the inherent challenges in the area of WSN. Many WSN applications are based on secure group communication. Authentication is one of the very effective ways to forestall unauthorized and corrupted communications from being forwarded in wireless sensor networks (WSNs). Because of this, many message authentication schemes have been developed, based upon either symmetric-key cryptosystems or public-key cryptosystems. Many of them, yet, have the limitations of high computational and communication expense in addition to absence of scalability and strength to node compromise problems. To address these issues, we propose Diffie-Hellman key exchange protocol. So, the security of the key distribution and management in wireless sensor networks will get solved by this method.

VI.REFERENCES

[1]. Ahmed, Khandakar, and Mark A. Gregory. "Integrating Wireless Sensor Networks with Cloud Computing." In *MSN*, pp. 364-366. 2011.

[2]. Botta, Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. "On the integration of cloud computing and internet of things." In *2014 International Conference on Future Internet of Things and Cloud*, pp. 23-30. IEEE, 2014.

[3]. Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of network and computer applications* 34, no. 1 (2011): 1-11.

[4]. Takabi, Hassan, James BD Joshi, and Gail-Joon Ahn. "Security and privacy challenges in cloud computing environments." *IEEE Security & Privacy* 8, no. 6 (2010): 24-31.

[5]. Wang, Cong, Qian Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving public auditing for data storage security in cloud computing." In *2010 proceedings ieee infocom*, pp. 1-9. Ieee, 2010.

[6]. Yi Ren, Member, IEEE, Vladimir I. Zadorozhny, Senior Member, IEEE,Vladimir A. Oleshchuk, Senior Member, IEEE, and Frank Y. Li, Senior Member, IEEE, “A Novel Approach to Trust Management in Unattended Wireless Sensor Networks” IEEE transactions on mobile computing, vol. 13, no. 7, July 2014

[7]. V. C. Gungor, B. Lu, and G. P. Hancke, Oct. 2010 “Opportunities and challenges of wireless sensor networks in smart grid,” IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564.

[8]. J. Chen, X. Cao, P. Cheng, Y. Xiao, and Y. Sun, Dec. 2010 “Distributed collaborative control for industrial automation with wireless sensor and actuator networks,” IEEE Trans. Ind. Electron., vol. 57, no. 12, pp. 4219–4230.

[9]. X. Cao, J. Chen, Y. Xiao, and Y. Sun, Nov. 2010 “Building-environment control with wireless sensor and actuator networks: Centralized versus distributed,” IEEE Trans. Ind. Electron., vol. 57, no. 11, pp. 3596–3604.

[10]. Z-J Han, R-C Wang, and F. Xiao, “A Multicast Algorithm for Wireless Sensor Networks Based on Network Coding”, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, 2014.

[11]. Y. Han S. Chen W. Du, J. Deng and P. Varshney, “A key management scheme for wireless sensor networks using deployment knowledge,” in *Proceedings of IEEE Infocom*, Hongkong, China, 2004.