

Developing a Group-based Security Scheme for Wireless Sensor Networks

Md. Abdul Hamid, Md. Mustafizur Rahman, Young Jig Yoon, and Choong Seon Hong
Department of Computer Engineering, Kyung Hee University, 449-701, Korea
E-mail: {hamid,mustafiz,yjyoon}@networking.khu.ac.kr, cshong@khu.ac.kr

Abstract—This paper presents a group-based security scheme for distributed wireless sensor networks. The scheme is proposed with 3-types of entities: one or more base stations, Y number of group dominator nodes, and N number of ordinary sensor nodes. We model the group-based deployment using Gaussian (normal) distribution and show that more than 85% network connectivity can be achieved with the proposed model. The small groups with pre-shared secrets form the secure groups where group dominators form the backbone of the network. The scheme is devised for dealing with sensory data aggregated by groups of collocated sensors; i.e., local sensed data are collected by the dominating nodes and sent an aggregated packet to the base station via other group dominators. The scheme is shown to be light-weight, and it offers a stronger defense against node capture attacks. Analysis and simulation results are presented to defend our proposal. Analysis shows that robustness can significantly be improved by increasing the deployment density using both the dominating and/or ordinary sensor nodes.

I. INTRODUCTION

Wireless sensor networks (WSNs) are envisioned to be economic solutions to many applications as forest fire detection, battlefield surveillance, disaster management, homeland security operations, border control and so on [5], [6]. Generally, each sensor node in the network acts as an information source, sensing and reporting data from the environment for a given task. The low-cost sensors forward data to a querying sink/base station (BS). However, reporting sensing data is often unnecessary as in many cases sensors in an area detect the common phenomena. So there is a high redundancy in sensed data. Nevertheless, it is very inefficient for every single sensor to report their data back because every data packet traverses many hops to reach BS and nodes are stringent in resources (*e.g.*, memory, communication, computation and power).

Recently many data aggregation protocols [1], [2], [3], [4] have been proposed to eliminate the data redundancy in sensor data of the network, hence reducing the communication cost and energy expenditure in data collection. During a typical data aggregation process, sensors are organized into a tree hierarchy rooted at a BS. The non-leaf nodes act as aggregators, fusing the data collected from their child nodes before forwarding the results towards the BS. In this way, data are processed and fused at each hop on the way to the BS, and communication overhead can be largely reduced. In [9], an improved performance of the existing key-pre-distribution techniques has been presented using the locality of group deployment. The proposed framework in [9] does not require

the sensors' expected locations for key-pre-distribution. This paper presents a group-based deployment approach similar to the scheme in [9] to model the network. However, our approach differs from [9] as our primary goal is to deal with sensed information aggregated by groups of collocated sensors and to show the tolerance against node capture attacks. Network topology consists of heterogeneous entities: Base Station (BS), Group Dominator (GD), and ordinary Sensor Node (SN). To preserve the efficiency, our scheme performs data aggregation in each logical group and generates one aggregate from each group. After the BS has collected all the group aggregates, it then checks the validity of the carried MACs (Message Authentication Codes) in the reports and discards the forged report if any. Analysis and simulation results show the scheme's tolerance against increasing number of node compromise.

The rest of the paper is organized as follows. Section II presents related works. Deployment model and security aware data aggregation scheme are presented in Section III. Security analysis and simulation results are presented in Section IV. Section V concludes this work.

II. RELATED WORKS

In Eschenauer-Gligor scheme [10], a large key pool of n keys is generated. Then, m keys are randomly selected from the n keys and are distributed to each node. Therefore, any two nodes have one common key with a certain probability. For example, if $n = 10000$ and $m = 83$, the probability that two nodes have at least one common key is 50%. Moreover, with an increase in the size of the key pool (n), the number of keys stored by each node (m) should be increased to maintain a certain connectivity. For example, if $n = 100000$ and the required connectivity is 50%, m must be greater than 260. This value is too large for resource-constrained sensor nodes. The Du et. al. scheme proposed in [11] is one of the improvements of the Eschenauer-Gligor scheme. In this scheme, two nodes deployed to the same rectangle can share keys with a high probability because their subset key pools are the same. Two nodes deployed to neighboring rectangles share keys with a lower probability because their subset key pools have fewer common keys. If two nodes are deployed to non-neighboring rectangles, the probability of key sharing is zero. Therefore, the damage due to the compromise of one node is limited to neighboring rectangles, and hence, the network is resilient against node capture. This scheme assumes the group-

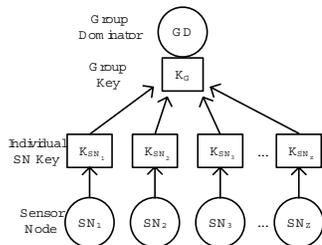


Fig. 1. Pre-distribution of initial secrets using star key graph

based deployment model, and the deployment points should be horizontal grid points. For other deployment models, dividing the deployment area and the subset key pool generation are not clearly described.

Public-key cryptography is a possible solution for key establishment in wireless networks. Though recent work [7] demonstrates cases in which public-key cryptography can be implemented on some resource-constrained devices, it is not yet feasible for all multi-hop networks. In the absence of public-key protocols, key establishment must be performed using symmetric keys which are assigned to nodes prior to network deployment, a solution known as key pre-distribution. Another extreme solution is the assignment of a global key to every node in the network. However, if an adversary is able to obtain the global key, the security of the entire network is compromised. A promising approach to symmetric key assignment which attempts to balance the trade-offs between complexity, storage and security is the star key graph based [8] key assignment. Through star key assignment, the complexity of public key protocols, the storage overhead of pair-wise key protocols and the easy compromise of global key protocols can be mitigated. Our scheme shows that each of the ordinary SNs needs to maintain only 3 keys. Furthermore, most solutions did not address node re-keying or security at different levels of granularity. Our solution, on the other hand, assigns different level of security loads according to resource capability and is applicable to members that are affiliated subgroups of nodes.

III. GROUP-BASED SECURITY SCHEME

In this section, we model the group-based security scheme. Prior to network deployment, initial secrets are assigned. Then the SNs are deployed into the area of interest and the secure group-based network formation is described. Post-deployment re-keying is presented at the end of this section.

A. Key Pre-distribution

In the offline key pre-distribution phase, we assign the group keys and individual keys to a group of nodes. For this, the key assignment is accomplished according to Fig. 1. Each GD holds the group key K_G and all the individual keys of SNs, $K_{SN_1}, \dots, K_{SN_Z}$, where Z is the number of ordinary sensor nodes in a particular group. Each SN holds group key K_G and its individual key K_{SN} shared with GD. There is also a shared key between BS and each SN and a shared key between BS and each dominating node (not shown in Fig. 1).

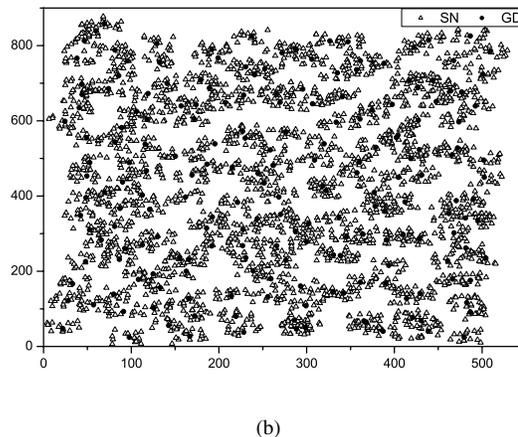
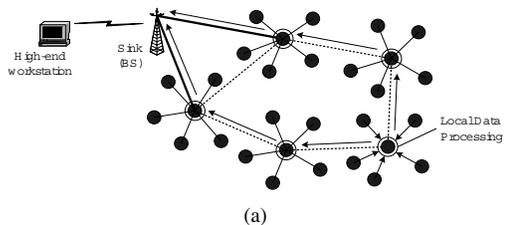


Fig. 2. Typical group-based deployment scenario: (a) Desired group-based topology, and (b) Observed topology from proposed deployment model

B. Network Model

We devise a 3-tier sensor network composing 3 types of nodes. The BS is considered as resourceful enough in terms of residual energy, computation power and speed, and communication. We assume that SN is simple, inexpensive and stringent in resources, while GD is rich in resources and more compromise-tolerant and having transmission range more than $2 * R_{SN}$, where R_{SN} is the transmission range of an ordinary SN. We also assume that one GD can communicate with its neighbor GD to forward aggregated messages towards the BS. The connectivity (and routing) from the sensor to the BS is dependent on the pre-distributed secrets. We assume that all the SNs and GDs are static after they are deployed in the deployment field. The final locations of the nodes differ from each other after the deployment. However, we assume that the final locations of a GD and its children SNs follow the same probability distribution function. The detailed deployment model is described below.

The GDs and SNs that are to be deployed are divided into n groups $\{G_i \mid i = 1, 2, \dots, n\}$ according to the group and sensor-GD pair-wise keys. A Single GD and Z SNs form a group. We assume that the groups are evenly and independently deployed on the targeted field. The nodes in the same group G_i are deployed from the same place at the same time with the deployment index i . During the deployment, the resident point of any node in group G_i follows a probability distribution function $f(x, y)$, which we call the deployment distribution of group G_i . The actual deployment distribution is affected by many factors. For simplicity, we model the deployment distribution as a Gaussian (Normal) distribution

TABLE I
CONNECTIVITY OF THE GROUP-BASED DEPLOYMENT MODEL

GD	SN	In Group	Out of Group	Out of Net	Connectivity
200	3000	2382	189	429	85.70%
300	3000	2371	197	432	85.60%
300	4500	3571	286	643	85.70%
300	6000	4719	421	860	85.60%

[9] since it is widely studied and proved to be useful in practice.

Let us assume that V_{BS} , V_{GD} and V_{SN} are the sets of BS, GD and SN respectively and $G(V, E)$ represents entire network in the graph model where, $V = \{V_{BS} \cup V_{GD} \cup V_{SN}\}$. The network backbone $G_B(V_B, E_B) \subseteq G(V, E)$ is formed by the GDs and BSs, provided that, all GDs present in the backbone have at least one path between each-other; i.e., each GD has a BS within its transmission range or has another GD that can communicate with any of the BS, and, at least one path exists between the backbone and a BS. The SNs form GD rooted local groups (Fig. 2) by pair-wise and group keys. Hence the connectivity between a SN and its parent GD depends on:

- i) $d(x, y) \leq R_{SN}$, where $x \in V_{SN}$, $y \in V_{GD}$, $d(x, y)$ is the distance between x and y , and R_{SN} is SN's transmission range, and,
- ii) $GroupKey_{GD} = GroupKey_{SN}$.

Fig. 2 shows typical group-based deployment scenario. In the figure, GD represents the local group dominator and SN represents the constrained SNs. SNs are connected locally to its GD and all GDs are connected network-wide (i.e., backbone network). The backbone network formed by GDs is connected to the BS and thus, the whole network is connected.

Table I shows the observed connectivity of proposed deployment model. We take different number of GDs and SNs with their group key and transmission range. More than 85% SNs fall within the overall network in which they are connected by their GD or other GD (out of group).

C. Secure Network Formation

After the deployment, each SN_i discovers its own GD_j . For this purpose, SN_i broadcasts an encrypted SN-JOIN-REQ (using individual key K_{SN_i}) message to all of the nodes within its transmission range. If the corresponding GD_j is within its transmission range (i.e., one hop distance), it gets the message and decrypts it as all the individual keys of the sub-ordinate nodes are known to the GDj. Upon successful decryption of the message, the GD sends a JOIN-APPROVAL message to the SN_i encrypting it with the group key (shared among SN_i in GD_j). Thus the SN_i becomes a dominated node of this corresponding GD_j . If, for any SN_i , the GD_j assigned during pre-distribution of keys, is not within one hop distance; the SN_i needs to inform the BS for resolving the issue. On discovering itself as out of its own GD, the SN_i sends a GD-ERROR message encrypting it with its individual key. This message is simply forwarded by other sensors and GDs in the network to reach to the BS. For resolving the unexpected issue of this kind, two special cases are considered.

Case I The SN has no dominator as its one-hop neighbor. In such a case, after getting the GD-ERROR message from the SN, the BS issues a command COMM-SN to assign the sensing role and to be connected with any SN within its vicinity. For sending the command, the BS uses the individual key of the SN. Employing this method keeps the isolated node connected with the rest of the network.

Case II The SN does not have its own GD within its one-hop neighborhood but another GD is available in the vicinity. Failing to find out its own GD, SN sends the encrypted GD-ERROR message to the BS. Now, as the GD of another group is present within its one hop distance, it gets the encrypted GD-ERROR message (only detects the type of message and just notes this incident), informs this message encrypted with its group key to the BS. The BS checks the message and issues a command COMM-AGD to that neighbor GD to be its adopter and also sends the individual key for this SN. The GD in turn uses this key to send its KG to the SN to welcome it in its own group. Thus, all the groups can form the overall network backbone where the GDs of the logical groups are the dominating nodes and all other nodes in the network are dominated.

D. Local Data Processing and Forwarding

If there are Z number of SNs in a group, for fidelity and correctness of data, the GD waits for the same sensing event from at least qq ($q \leq Z$) number of the SNs, where q is the threshold value set for a particular group. We consider any one group with ordinary SNs and its corresponding GD. Once an event occurs, q out of Z ($0 \leq q \leq Z$) sensors (ID_1, ID_2, \dots, ID_q) within the sensing area detect the event and send information to the GD. The message aggregation is accomplished in the following manner:

$SN_i \rightarrow GD_j : ID_i | E(M_i | MAC(M_i, K_{(SN_i, GD_j)}), K_{(SN_i, GD_j)})$
where, i^{th} SN belongs to j^{th} GD, $K_{(SN_i, GD_j)}$ is the shared key between SN and corresponding GD, $E(\cdot)$ is the encryption, and $|$ denotes bitwise XOR operation, and MAC is the message authentication code. Upon receiving the message sensed by SN_i , dominator GD_j verifies every single MAC and generates an aggregated report (and discards the false packet if any).

All the SNs in a particular group j also creates a MAC using the shared key between SN and BS and this MAC is only to be verified by the BS but to be relayed by its GD. The message format is: $SN_i \rightarrow GD_j : ID_i | MAC(K_{(SN_i, B)})$, where, $K_{(SN_i, B)}$ is the shared key between a SN and a BS. Now, GD collects all the MACs from SNs and sends q MACs, q IDs, ID_{GD_j} , and M_{GD_j} to the BS directly or via its neighboring GD as follows

$GD_j \rightarrow Sink : ID_{GD_j}, E(K_{(GD_j, B)}, ID_{GD_j} | M_{GD_j} | MAC_{(SN_1, B)} | \dots | ID_q | MAC_{(SN_q, B)})$.

The q MACs and an aggregated report M_{GD_j} are sent securely to the BS. Upon receiving the report, the BS first decrypts the message using the corresponding key $K_{(GD_j, B)}$, then it checks whether the report carries at least q distinct

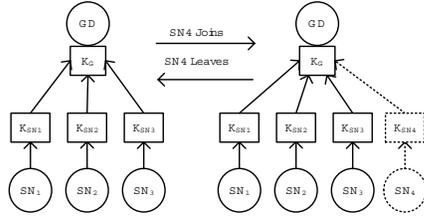


Fig. 3. Re-keying mechanism in a local group (node join/leave)

MACs from SNs and whether the carried MACs are the same as the MACs it computes via its locally stored keys. If no less than q MACs is correct, the event is accepted to be legitimate; otherwise it is discarded.

E. Post-deployment Re-keying

When any new node is deployed, it sends the JOIN-REQ-NEW message using its own individual key and, if authorized by the access list of GD, it joins the group. Otherwise, GD forwards this to BS. BS informs GD about the individual key of that SN. If authenticated by BS, GD generates a new group key and encrypts the new group key with the newly added node's individual key and sends it to the SN. For example, let's say, SN_4 in Fig.3 wants to join the existing group. GD changes the group key K_G to a new key $K_{G_{new}}$, and encrypts it with the old group key and sends $GD_j \rightarrow allSN_i : E_{K_G}(K_{G_{new}})$ to all sensors. And GD encrypts new group key with the joining SN's individual key and sends $GD \rightarrow SN_4 : E_{K_{SN_4}}(K_{G_{new}})$. Similarly, when any SN wants to leave the group, it just sends a leave message, $SN_4 \rightarrow GD : E_{K_{SN_4}}(leave)$. Upon receiving the leave message, GD deletes the leaving SN_4 and updates the K_G to a new $K'_{G_{new}}$, encrypted with remaining SN's individual key and unicasts the message $GD \rightarrow SN_{i-1} : E_{K_{SN_{i-1}}}(K_{G_{new}})$. In this way, the key management for a new node join/leave can be handled.

IV. SECURITY ANALYSIS

We contemplate on analyzing the threat posed by compromising the SNs and GDs. An adversary may jeopardize the network in the following ways: First, an adversary can simply deploy some malicious SN into a group. A malicious sensor without having the secret key may try to produce a false sensing result with an identity of a legitimate sensor. Since, a malicious SN does not have the capability of producing a valid MAC for the false sensing result, the GD will identify it. Second, an adversary can copy some SNs from some group and deploy them into another group. As each GD knows the set of SNs within its own group, a GD is able to identify an illegitimate ID of ordinary SN. Nevertheless, a compromised SN can not fool the GD of another group without knowing the valid key. Similarly, a compromised GD from one group does not fool the SNs of another group without knowing the valid keys. Third, given any group having a GD and Z SNs, an adversary may launch attack in three ways: (a) compromise some SNs only, (b) compromise the GD only,

and (c) compromise the GD and some SNs concurrently. We term this security threat as intra-group node capture. And fourth, an adversary may launch attack in a distributed manner: (a) randomly compromise SNs throughout the entire network and/or (b) intelligently compromise few GDs where maximum number of SNs has already been captured. We term this security threat as network-wide node capture. In the rest of this section, we analyze intra-group and network-wide node capture attacks.

A. Intra-group Node capture

1) *Ordinary sensor nodes are captured:* A compromised ordinary sensor in a particular group may produce an invalid MAC by providing wrong guarantee for an aggregated report. The group-based scheme is robust against this kind of attack as long as no more than q sensors within a local group are compromised. Since we devise our scheme where each aggregated report carries q number of MACs from sensors.

2) *Only the group dominator is captured:* When a GD is captured, it may fabricate a report. But to do that, at least q MACs need to be forged. The probability that at least q out of Z MACs is correct is given by $p_{GD} = \sum_{j=q}^Z \binom{Z}{j} p^j (1-p)^{Z-j}$, where, $p = 1/2^L$ and L is the MAC size in bits. It can be seen that this probability p_{GD} is negligible for 4-byte CBC MAC [14]; moreover, only one group out of the entire network is in fact affected while other groups are not.

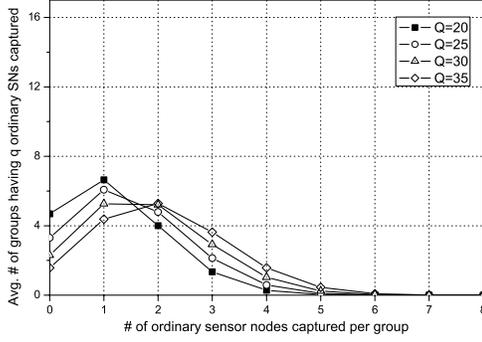
3) *Group dominator and sensor nodes are captured:* We consider the situation where an adversary has compromised a GD and some number x ($0 \leq x \leq q$) SNs concurrently. To inject a false report, a GD needs at least q valid MACs. Since a GD has to forge $(q-x)$ more MACs, the probability that $(q-x)$ out of $(Z-x)$ is valid, is given by $p_{GD}^x = \sum_{j=q-x}^{Z-x} \binom{Z-x}{j} p^j (1-p)^{Z-x-j}$. Again, this probability is almost negligible [14]. If an individual key is compromised, the attacker at best could send false report to the GD but when any message from the GD comes encrypted with the group key, it cannot decrypt it.

B. Network-wide Node Capture

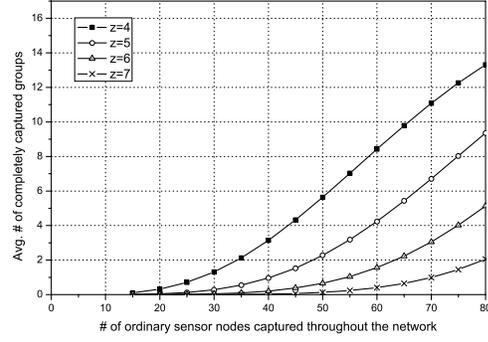
We analyze the robustness of our scheme when an adversary has randomly compromised Q ($0 \leq Q \leq N$) ordinary SNs and j ($0 \leq j \leq Y$) GDs from the entire network. Let $p(j, q)$ be the probability that j^{th} GD (i.e., j^{th} group) having q ($0 \leq q \leq Z$) SNs compromised, we get

$$p(j, q) = \binom{Z}{q} \binom{N-Z}{Q-q} \div \binom{N}{Q} \quad (1)$$

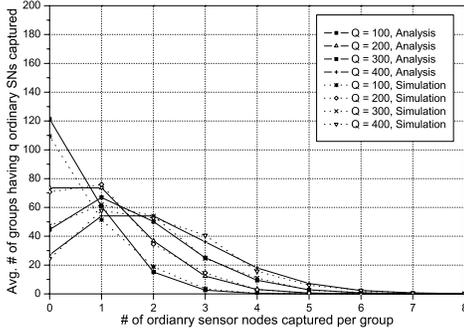
We define $g(j, q) = 1$ if SNs are captured in j^{th} group, 0 otherwise. Let G_q denote the number of groups having q ordinary SNs captured from the entire network, we get $G_q = \sum_{j=1}^Y g_{j,q}$, and the expected number of groups having



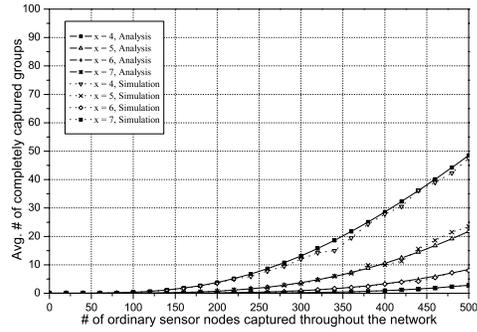
(a) Avg. No. of groups having q SNs captured



(b) Avg. No. of completely captured groups



(c) Avg. No. of groups having q SNs captured



(d) Avg. No. of completely captured groups

Fig. 4. Security Analysis: (a), (b) Quantitative ($N = 170, Y = 17, Z = 10$), and (c), (d) Poisson Analysis and Simulation ($N = 3000, Y = 200, Z = 15$)

q ordinary SNs captured can be calculated as (2).

$$E[G_q] = \sum_{j=1}^Y E[g_{j,q}] = Y \cdot E[g_{j,q}] = Y \cdot p(j, q) \quad (2)$$

Next, we assume that an adversary has captured some groups having the z ($z \geq q$) SNs compromised and we call this situation as a complete group capture. Let X be the number of completely captured groups from the entire network. We can compute $E[X]$ by equation (3) as:

$$E[X] = \sum_{q=z}^Z G_q = \sum_{q=z}^Z Y \cdot p(j, q) \quad (3)$$

For demonstration purpose, we take a simple example where total number of SNs is $N = 170$, with $Z = 10$ SNs in each group (i.e., $Y = 17$ groups). Fig.4a shows the expected number of compromised groups against the entire network's compromised ordinary SNs. When 20 SNs are captured, 5 groups having 0 SNs compromised and only 1 group having 3 SNs compromised. Fig.4b demonstrates the number of fully compromised groups that depends on the value z . Four cases are shown when z is 4, 5, 6 and 7. When z is 4, 3 (16.66% of entire network) groups are fully compromised against 40 (23.5%) compromised SNs. But, as the value of z increases (e.g., 6 or 7), number of fully compromised groups are

much smaller. We observe that robustness can be improved significantly by increasing the value of z .

Next, we use the properties of Poisson Process to analyze the robustness of our scheme. We consider the case where the number of compromised SNs Q is much less than the total number of SNs N (i. e. $Q \ll N$). We denote the status of any sensor in a particular group as C_i , for $i = 1, 2, \dots, Z$ and consider it as Bernoulli random variable. Let $C_i = 1$, if the i^{th} sensor is captured and $C_i = 0$, if not captured. Considering the Q captured SNs are uniformly distributed across the network, probability of any SN captured by an adversary can be given by $p[C_i = 1] = Q/N, i = 1, 2, \dots, Z$. If the condition $Q \ll N$ holds, then, C_1, C_2, \dots, C_Z are said to be independent according to the properties of Poisson Process [13] and the number of captured sensors in a particular group follows the Poisson distribution with approximated mean value Q/Y . So, if q sensors are captured in a group, we get the probability as $p[q] \approx e^{-Q/Y} \frac{(Q/Y)^q}{q!}$. Now, if the total number of groups is Y , we calculate the expected value of the number of groups Y having q sensors captured as (4):

$$E[Y_q] \approx Y \cdot e^{-Q/Y} \frac{(Q/Y)^q}{q!} \quad (4)$$

Next, considering the case where an adversary has captured some groups having the x ($x \geq q$) SNs captured and we call this situation as complete group capture. Let X be the number

V. CONCLUSION

We have proposed a group-based secure network where dominating node processes sensed information locally and prepares the authenticated report for the destination. The star based key pre-assignment has significantly less storage overhead, and the analysis and simulation results show that group-based architecture is strongly resilient to node capture attacks. Further, the robustness capability of the group-based network manifests itself not only in the number of sensor nodes, but also in the number of superior group dominating nodes. The proposed model implicates that nodes can be grouped into small clusters or cells where in each cell one can designate a specific node to carry all the burden of relaying multi-hop packets. Thus a division of labor is possible to make the overall scheme to be profitable by reducing transmission power consumed by the vast majority of other ordinary nodes. Future works include the effect on end-to-end delay and energy consumption incurred by the security protocol.

ACKNOWLEDGMENT

This research was supported by the MIC under the ITRC Project supervised by the IITA.

REFERENCES

- [1] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in Proc. of ACM Mobicom, Seattle, Washington, USA, August 1999, pp. 263-270.
- [2] C. Intanagonwiwat, D. Estrin, R. Govindan, and J. Heidemann, "Impact of network density on data aggregation in wireless sensor networks," in ICDCS, 2002, pp. 457-458.
- [3] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in MOBICOM, 2000, pp. 56-67.
- [4] B. Krishnamachari, D. Estrin, and S. Wicker, "The impact of data aggregation in wireless sensor networks," in Intl. Workshop on Distributed Event-Based Systems, (DEBS 02), Vienna, Austria, July 2002.
- [5] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on sensor networks," IEEE Communications Magn, vol. 40, no. 8, 2002.
- [6] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, March 2002.
- [7] N. Gura, A. Patel, A. Wander, H. Eberle, S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in Proc. of the Sixth Workshop on Cryptographic Hardware and Embedded Systems (CHES04), Cambridge, MA, USA, 2004, pp. 119-132.
- [8] C. K. Wong, M. Gouda and S. S. Lam, "Secure Group Communications Using Key Graphs," IEEE/ACM Trans. on Networking, Vol. 8, No. 1, February 2000.
- [9] Donggang Liu, Peng Ning, and Wenliang Du, "Group-Based Key Pre-Distribution in Wireless Sensor Networks," in Proc. ACM WiSE05, September 2, 2005.
- [10] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. of the 9th ACM Conference on Computer and Communications Security, November 2002, pp. 41-47.
- [11] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in Proc. of the IEEE INFOCOM, March 2004, pp. 586-597.
- [12] G.J. Pottie, and W.J. Kaiser, "Wireless integrated network sensors," Communications of the ACM 43 (5) (2000), pp. 551-558.
- [13] S. M. Ross, *Introduction to Probability Models*, Academic Press, 2003, 8th Edition.
- [14] Y.W. Law, J. Doumen, and P. Hartel, "Survey and benchmark of block ciphers for wireless sensor networks," ACM Trans. on Sensor Networks, vol. 2, no. 1, February 2006, pp. 65-93.

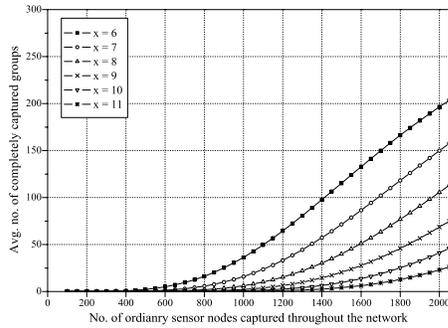


Fig. 5. Impact of deployment density ($N = 6000, Y = 300, Z = 20$).

of completely captured groups from the entire network. We can compute the expected value $E[X]$ by:

$$E[Y_q] \approx \sum_{q=x}^Z Y_q \approx \sum_{q=x}^Z Y \cdot e^{-Q/Y} \frac{(Q/Y)^q}{q!} \quad (5)$$

Robustness against node compromise has been plotted in Fig. 4(c) and 4(d) using the analytical result calculated from Poisson Process as well as the results obtained by simulation. The results are almost similar as can be seen in Fig. 4(c) and (d). Fig. 4(c) shows the average number of groups where $q(0 \leq q \leq Z)$ ordinary SNs are compromised by the attacker in each individual group. 37 groups having 0 and 18 groups having 2 SNs compromised when $Q = 100$ SNs are captured from the entire network. In worst case, when 400 SNs are capture network-wide, only 18 groups out of 100 having 4 SNs captured. Fig. 4(d) shows the average number of groups that are fully captured when more than $q(q \leq x \leq Z)$ sensor nodes are captured. For the values x equals 4, 5, 6 and 7, we realize that for $x = 4$, 73% groups are fully captured when 25% SNs are captured throughout the network. But, as the value of x increases, its robustness gets stronger. For example, $x = 7$, 23% (23 out of 100) groups are captured for 25% (500 out of 2000) network-wide captured SNs. So, significant improvement in network robustness can be achieved by increasing the value of x .

Fig. 5 plots our analysis when the deployment density is increased in terms of ordinary SNs and GDs. Poisson analysis reveals the fact that the expected number of groups having q ordinary SNs captured in each group is independent on the low and high deployment density. However, the effect on the complete group compromise is significant. It can be seen from Fig. 5 that when $x = 10$, and $Q = 1000$ (i.e. 16.66%) ordinary captured nodes leads to only 0.70 (i.e. 0.23% of entire groups) groups to be completely captured. Hence, robustness may significantly be enhanced by increasing the number of SNs as well. Interested readers may verify that network robustness can also be improved by increasing the number of group dominators.