효율적인 안전한 유비쿼터스 센서 네트워크를 위한 하이브리드 방식의 아이디 할당

IDs Assignment of Hybrid Method for Efficient and Secure USN (Ubiquitous Sensor Networks)

성 순 화*
Soonhwa Sung

요 약

이동 에드 혹 네트워크와 센서 네트워크의 차이 때문에 이동 에드 혹 네트워크를 위한 pre-existing autoconfiguration를 센서 네트워크에 간단히 적용할 수 없다. 그러나, 아직 지역적으로 효과적인 유일한 주소 할당이 필요한 메커니즘이 있다. 본 논문은 지역적인 센서 네트워크의 하이브리드 방식의 아이디 할당 계획안을 제안한다. 이러한 하이브리드 방식은 proactive IDs assignment와 reactive IDs assignment를 결합한 방식이다. 제안된 계획안은 reactive IDs assignment을 사용하여 효율적인 통신을 고려하고, zone-based self-organized clustering with Byzantine Agreement를 사용하여 공격에 대한 안전을 고려한다. 따라서 본 논문은 네트워크 트래픽을 최소화하고 센서 네트워크의 이탈한 노드로부터 네트워크를 회복하는 문제를 해결한다.

Abstract

Due to the differences between a mobile ad-hoc network and a sensor network, the pre-existing autoconfiguration for a mobile ad-hoc network cannot be simply applied to a sensor network. But, a mechanism is still necessary to assign locally unique addresses to sensor nodes efficiently. This paper proposes a hybrid IDs assignment scheme of local area sensor networks. The IDs assignment scheme of hybrid method combines a proactive IDs assignment with a reactive IDs assignment scheme. The proposed scheme considers efficient communication using reactive IDs assignment, and security for potential attacks using zone-based self-organized clustering with Byzantine Agreement in sensor networks. Thus, this paper has solved the shortage of security due to minimizing network traffic and the problem of repairing the network from the effects of an aberrant node in sensor networks.

☞ Keywords: hybrid IDs assignment, reactive IDs assignment, proactive IDs assignment, Byzantine Agreement Protocol of Proactive AVSS, sensor networks

1. Introduction

In recent years, an exciting new type of networks has called sensor networks[1,2]. Contrary to more traditional computer networks, these sensor networks consist of a large number of ultra-small autonomous devices. Each device, called a sensor node, is battery powered and equipped with integrated sensors, data processing capabilities, and short-range radio communication[3].

A sensor network consists of a large number of sensor nodes engaged in environment monitoring and wireless communications, simultaneously. Due to the low cost of a sensor node and the convenience of deployment, a sensor network will find applications in many areas, such as battlefield surveillance, precision agriculture, smart transportation, and wildlife study[4]. Although a sensor network is similar to a MANET since both are multi-hop wireless networks, they are different in their architectures and data communication

* 종신회원 : 충남대학교 전기정보통신공학부 BK교수
shsung@cnu.ac.kr
[2008/03/05 투고 - 2008/03/12 심사 - 2008/06/24 심사완료]

schemes. A MANET is usually an IP-based network, and any node in the network can initiate communications with any other node. Thus, every node must be assigned an IP address that is globally unique. To initiate data communications, the IP address of the destination must be identified and the path to it must be built.

Without the IP routing function provided by the IP layer, a node in the sensor network still needs an approach to find the path toward the destination. The directed diffusion paradigm[5] was proposed to replace IP routing for data communication in sensor networks. According to the scheme, a sink node broadcasts an interest message that is flooded throughout the network. Every node records the upstream node as the next hop towards the sink. After the path is built, the reply is sent back from the source along the reverse path to the sink. The sink node and source nodes can reinforce the path, so subsequent queries can be unicast packets[4].

Although there have been many autoconfiguration algorithms proposed for IDs assignment in MANETs [6-8], they aim at the assignment of globally unique IP addresses to nodes in the network, and are not appropriate for IDs assignment in a sensor network due to the following reasons:

1. The number of nodes in a sensor network is very large, so the probability of duplicate address may be very high with a limited number of address bits. Thus, high communication overhead will occur to achieve global uniqueness.
2. Most of the nodes in a sensor network join the network and require IDs almost at the same time because they start up simultaneously after deployment.
3. It is meaningless to achieve the global uniqueness of IDs of the sensor nodes, since an IP address is not used in the sensor network. Therefore, locally unique IDs will suffice for the directed diffusion communication model.
4. The size for the address field(payload length) should be very small in a sensor network. Otherwise, data communications will be less efficient.

Although all the sensor nodes may be equipped with a locating device such as GPS(Global Positioning System), it is not adequate to simply use the location of a sensor node or the hash value of the location information as its IDs because:

1. The number of bits to require the location information in the address field may be large, so considerable power will be wasted.
2. The nodes of sensor networks with high node density may have the same location information due to the low resolution of the locating device.
3. Without comparision, the hash value of the location informationis still unknown if the hash values of adjacent nodes are different or not[9].

On the other hand, the nodes of sensor networks require to be secure. Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, non-repudiation, and anti-playback. In the case of sensor network, a security is required for authentication, integrity, privacy(or confidentiality), non-repudiation, and anti-playback. The recipient of a message needs to be able to be unequivocally assured that the message came from its stated source. Similarly, the recipient needs to be assured thatthe message was not altered in transit and that is not an earlier message being re-played in order to veil the current environment. Finally, all communication need to be kept private so that eavesdroppers can not intercept, study and analyze, and devise countermeasures in order to circumvent the purposes of the sensor network.

Secure sensor technology is to provide privacy and integrity to the data, to authenticate the sender, to prevent replay attacks and to prevent traffic analysis. Consequently, the entire communication is encrypted, but must minimize network traffic.

The typical security problems in sensor networks are as follows:

1. Passive information gathering: If communications between sensors are in the clear, then an intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. If information has to be encrypted, then "how" is the open question. In other words, which cryptographic approaches will be best, given the resource constraints and the routing paradigm employed by the sensor?
2. Subversion of a node: A particular sensor might be "captured", and information stored on it(such as the key) might be obtained by an adversary. If a node has been compromised then how to exclude that node, and that node only, from the sensor network is at issue. The smart card community has done significant work to address such situations that may be adapted to the security solutions for sensor networks.
3. False node: An intruder might "add" a node to the system that feeds false data or prevents the passage of true data. While such problems with malicious hosts have been studied in distributed systems, as well as ad-hoc networking, the solutions proposed there(group key agreement, quorums and per hop authentication) are in general too computationally demanding to work for sensors.
4. Legitimate addition of a node to an existing sensor network: If a node needed to be replaced or another node needed to be added to an existing sensor network, securely integrating the new node into the existing network is at issue[10].

These problems in sensor networks were solved by the security protocol in [10]. But [10] has not implemented the protocol to repair the network from the effects of an aberrant node. The proactive IDs assignment scheme for a solution of this problem, and the reactive IDs assignment scheme for improvements of traffic and power consumption problems in USN are presented in this paper. That is, this paper proposes the hybrid IDs assignment scheme which combines a proactive IDs assignment with a reactive IDs assignment scheme.

2. Related Works

2.1 Proactive IDs assignment Scheme

The Proactive IDs assignment Scheme motivates the security problem that sensor networks face by developing a scheme representative of a large application class where micro sensor networks would be used in the future.

The networked node of large networks, such as a sensor network, is usually unknown, since a sensor network is always dynamically changing as followings: new nodes are always added to the network, some nodes are down. But the traditional work on the Byzantine faults[11,12] covers only the case that the network is known. When the network is unknown faulty nodes cannot only send faulty data, but these can also pretend that bogus nodes and bogus edges exist [13].

Therefore, the scheme is focused on developing scheme to deal with Byzantine faults in sensor network without a trusted central certification authority. Because a new node joining a wireless sensor network needs to efficiently and automously set up secret keys with his communication partners without the use of a central infrastructure.

2.2 Byzantine Agreement Protocol with Proactive AVSS

Byzantine Agreement uses the following Byzantine adversaries that may alter the behavior of the corrupted parties in an arbitrary and coordinated way. A standard formulation of the Byzantine Agreement problem follows: design a protocol that allows the corrupted parties to agree on a common value. The agreed value should be the input value of one of the uncorrupted parties.

The scheme briefly explains how the use of homomorphic secret sharing is useful towards achieving proactive threshold cryptography.

The scheme assumes that the secret sharing scheme is homomorphic. If (s_1, s_2,…,s_l ℓ : the number of shareholders) is a share assignment for the key *k* and (s_1, s_2,…,s_l) is a uniformly random share assignment for the "key" 0, then (s_1, s_2,…,s_l)=(s_1+ s_1, s_2+ s_2 ,…, s_l+ s_l) is a new share assignment for the same key *k*. Assume that one trusts *t* shareholders. Then *t* participants, denoted by *j*, can each contribute their own random ($s_{j,1}$, $s_{j,2}$, …, $s_{j,l}$) When working in an Abelian group and when the secret sharing scheme is perfect, the resulting share s_i=s_i +$\sum_{j\in B} s'_{j,i}$ will be guaranteed independent of the original share s_i, due to the properties the one-time-pad. Both s_i and s_i are shares of the same key *k*.

Proactive AVSS(Asynchronous Veriable Secret Sharing) scheme consists of two protocols: Sharing protocol(S), Reconstruction protocol(R). The sharing protocol consists of three stages:first, each party waits to receive its share of the secret from the dealer. Next, the parties jointly try to verify that their shares define a unique secret. Once a party is convinced that a unique secret is defined , it locally computes and outputs a corrected share of the secret using the information gathered in the verification stage. In the reconstruction protocol, each party sends its share to the parties in some predefined set R(the set R is an external parameter with the same role). Next, each party in R waits to receive enough shares to uniquely determine a secret, and outputs the reconstructed secret. In order to deal with possibly erroneous shares(in $\sum_{j\in B} s'_{j,i}$), our scheme uses a algorithm for error correcting of a new Reed-Solomon code based on Newton's Interpolation. Thus the scheme has no probability of error and zero delay in reconstructing[13].

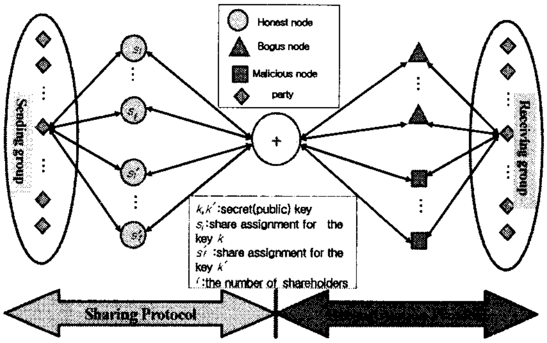
Honest node
Bogus node
Malicious node
party
Sending group
Receiving group
s_i
s_i
s'_i
s'_i
+
k,k' :secret(public) key
s_i :share assignment for the key k
s'_i :share assignment for the key k'
ℓ :the number of shareholders
Sharing Protocol

Fig. 1. Byzantine Agreement Protocol of Proactive AVSS

Therefore we can communicate securely even if there are the corrupted parties included malicious and bogus nodes in a wireless sensor network. That is, the scheme has solved the problem[10] repairing the network from the effects of an aberrant node in sensor networks.

2.3 Reactive IDs assignment Scheme

The reactive IDsassignment scheme has presented in [9]. The scheme can be applied to mobile sensor networks as well. As the sensor nodes move around, there will still be local ID conflicts after previous conflict resolution. However, as long as there is no data communication, the ID conflict brings no harm to the sensor network, and it will be resolved during the next data communication.

The reactive IDs assignment scheme[4] postpones ID conflict resolution until a communications are initiated. So, it contributes to save a communication overhead.

However, every node can not choose a random ID in the beginning. Because a sensor network consists of a large number of sensor nodes simultaneously engaged in monitoring environment and wireless communications.

The distributed IDs assignment is proposed in [14]. In order to assign ID, tree structure is used to compute the size of the network. Then unique IDs are assigned using the minimum number of bytes. However, this scheme uses not only assigning temporary ID and final unique ID but also obtaining sub-tree size. In order to assign temporal ID and final unique ID, high communication cost is needed.

[15] proposed an addressing scheme for cluster-based sensor networks. To prevent collisions, nodes within the same cluster are assigned different local addresses. However, the scheme has the energy cost of using global IDs in the case of large sensor networks. In addition, the proposed solution can be used only with cluster-based routing and does not extend to the case of multi-hop routing[16].

3. IDs Assignment Scheme of Hybrid Method

The proposed IDs assignment scheme of hybrid method combines a proactive IDs assignment with a reactive IDs assignment. The proactive IDs assignment supplies lack of security, and the reactive IDs assignment provides less traffic and power consumption in a sensor network.

3.1 Assumption

We define some assumptions like below.

1. The nodes in a sensor network initially begin to communicate in zone-based self-organized clustering with Byzantine Agreement.
2. The size of a zone should be less than threshold(t)
3. ID assigned field is combined as 2parts: Zone ID, Cluster head ID
4. The entire nodes in a zone only work during all its lifetime
5. The nodes of a cluster with an unique cluster head ID must communicate with Byzantine Agreement.

3.2 Zone-based Self-organized Clustering Algorithm

The algorithm is a distributed algorithm which each zone executes the algorithm independently and the failure of one zone does not affect the rest of the network. Zone building with IDs, zone$_i$(ID$_i$), has cluster G$_i$ with sequential cluster reformations. Cluster G$_i$ has the nodes with one cluster head of unique ID. Zone-based clusters delegates the nodes in each cluster as requirements. Security of zone building with IDs complies with byzantine agreement protocol.

Therefore, zone-based clusters do not broadcast their informations to nodes in an entire sensor network while they need to communicate each other. Securely, they broadcast their informations only to the nodes in zone-based cluster when they are required to communicate, so the interference in a zone with unique ID is less than it of traditional self-organized cluster.

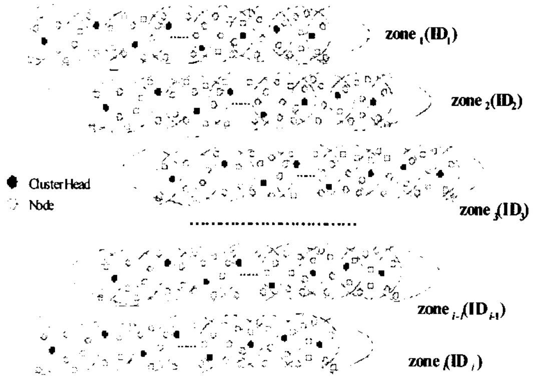

Fig. 2. Zone building with IDs

The algorithm executes in five consecutive phases.

Phase 1:

After power-on, listen for beacon signals from cluster heads. If, after a period of time t_b, no signal is received, they begin to transmit beacons themselves in random time slots at a pre-defined power level. Nodes that receive signals from other nodes in a zone with unique ID measure their distances to the neighboring nodes and calculate the interference factors. If a node receives signals from more than N_u neighboring nodes, only the closest N_u nodes are picked as neighbors. If a node waits for a period of time t_w without detecting a new neighbor, this node assumes that it has detected all of its neighbors in a zone with unique ID and goes to Phase 2. t_w is a parameter that needs to be optimized to reduce waiting time.

Phase 2:

Each node in a zone broadcasts its information, including its interference factor, node ID, zone ID and a list of neighboring nodes, to other zones in MANET. Each zone also maintains a table that contains information received from other zone. Again, if a zone waits for a period of time T without receiving new information, it assumes the broadcasting has completed and goes on to Phase 3.

Phase 3:

Once broadcasts have completed in a zone, all nodes that can be reached by one or multiple hops will have tables with entries from other nodes that can be reached in a zone. Each node that has a table should perform the following operations. N in a zone is the number of entries in the table.

For i=1 to N

1) Find the node with the minimum interference factor in the table and mark it as a cluster head.
2) Delete the cluster head's neighboring nodes in a zone from the table
3) Stop the iteration when there are no more cluster heads to pick.
4) If the iteration stops in a zone, the size of zone is threshold(t).

It should be noticed that without information losses, each node that can be reached by one or multiple hops should have the same table.

Phase 4:

Nodes that are marked as cluster heads in Phase 3 become the self-claimed cluster heads in a zone and start to send beacons.

Phase 5:

Each remaining node picks the closest cluster head, joins the cluster, and makes a zone. Once every node belongs to at least one cluster, nodes belonged to at least one cluster delete due to reforming in zone with unique ID[17].

3.3 Procedures

The procedures work for a random zone in a sensor network.

The hybrid IDs assignment algorithm works as follows:

1. Every cluster head in sending group(zone) chooses a random ID.
2. Generate a secrete key *k*, public key *k* for a random ID.
3. The sink node(cluster head) introduces to share assignment for the secret key *k* (don't consider public key *k*).
4. The sink node broadcasts an INTEREST message sharing assignment for the secret key *k* .
5. All the neighbor cluster heads record the sender's ID. If the sender's ID is the same as its own, it chooses another one randomly, and broadcasts a CHANGE message sharing assignment for the secret key *k* .
6. The neighbor waits for a random delay and rebroadcasts the INTEREST message.
7. If a cluster head receives an INTEREST message with the same source ID more than once, it puts the ID in a RESOLVE message sharing assignment for the secret key *k*, and broadcasts to its neighbors.
8. If a cluster head receives the RESOLVE message containing its ID, it chooses another one randomly, and broadcasts a CHANGE message sharing assignment for the secret key *k* .
9. After the intended source node(cluster head) receives the INTEREST message, it unicasts a REPLY message sharing assignment for the secret key *k* back to the sink.

The clusters of sending group have to share assignment of the secret key *k* for an unique cluster head ID. The sharing assignment for the secret key *k* uses Byzantine Agreement protocol of proactive AVSS.

3.4 Verifiable Secret Scheme

The network node of large networks such as a sensor network, is usually unknown, since a sensor network is always dynamically changing. When the network is unknownfaulty nodes not only send faulty data, but these can also pretend that bogus nodes and bogus edges exist. Therefore, the scheme is focused on developing scheme to deal with Byzantine faults in sensor network without a trusted central certification authority.

Because a new node joining the wireless sensor network needs to efficiently and automously set up secret keys with his communication partners without the use of a central infrastructure.

On the other hand, Byzantine Agreement can certificate transmission nodes in a network, but it cannot certificate the nodes which can bea source node as well as a sink node in sensor netwoks. Because any node in sensor networks can be a source node. Therefore, this scheme introducesthe zone-based self-organized clustering with unique IDs. This clustering can communicate securely even if the nodes in sensor networks is threatened by corrupted nodes. Because the clustering in sensor networks already identifies with unique IDs before a communication.

The clusters of sending group share assignment for the secret key k and public key k with l(the number of shareholders), and the sharing protocol broadcasts all clusters in a zone with unique ID. If there are bogus clusters or malicious clusters in a zone, reconstruction protocol broadcasts all clusters in a zone. Therefore, a coordinator of zoning process can communicate securely even if there are the corrupted nodes in sensor networks.

The scheme has two phases to verify secret plans: sharing phase and reconstruction phase.

■ Sharing Phase

1. Protocol for dealer on input a secret s
   - Randomly choose polynomials $f(x)=a_tx^t+\dots+a_1x+s$: s(shared secret value), and $r(x)=r_tx^t+\dots+r_1x+r_0$, $r(x)$: random string for sharing .
   - Compute and hand player P_i the values

     $\alpha_i \overset{def}{=\!=} f(i)$ and $\rho_i \overset{def}{=\!=} r(i)$, for $1 \le i \le n$
   - Computeand broadcast the value

     $A_i \overset{def}{=\!=} C(\alpha_i, \rho_i)$, for $1 \le i \le n$

     $C(\ f(i),\ r(i)\ )$: commitment function, $C\ (x,\ r)$: similar to SHA(Secure Hash Algorithm)-1

2. Player P_i verifies that $A_i = C(\alpha_i, \rho_i)$.

   If the equation does not hold then he broadcast a complaint against the dealer.

3. If Player P_i broadcasted a complaint then the dealer broadcasts the values

   α_i, ρ_i, s.t. $C(\alpha_i, \rho_i) = A_i$

4. If the Dealer does not follow some step he is disqualified, otherwise conclude that a secret has been shared.

■ Reconstruction Phase

1. Each player broadcasts the values α_i, ρ_i.
2. Take t+1 broadcasts the values for which A_i = $C(\alpha_i,\ \rho_i)$ and interpolate polynomials $\overline{f}\,(x)$ and $\overline{r}\,(x)$ of degree at most t that pass through those points.
3. Compute $\overline{\alpha}_i = \overline{f}\,(i)$ and $\overline{\rho}_i = \overline{r}\,(i)$ and verify that $C(\overline{\alpha}_i,\ \overline{\rho}_i)$ for all i.

If yes, output $\overline{f}\,(0)$ else output 0.

4. The Simulations

The simulations for the hybrid IDs assignment scheme are implemented to compare their performance in ns-2(version 2.27)[18]. A simple simulation scenario is run to verify the correctness of the implementation, which has 15 nodes in a 53 grid, as illustrated in Fig.3. The numbers shown in the figure are the unique IDs(UID) of the nodes(cluster heads), which are used for analysis only and should not appear in reality. The distance between two nodes is 200 m so that a node in the middle of the network has 4 direct neighbors. The size for the address is 4 bits.

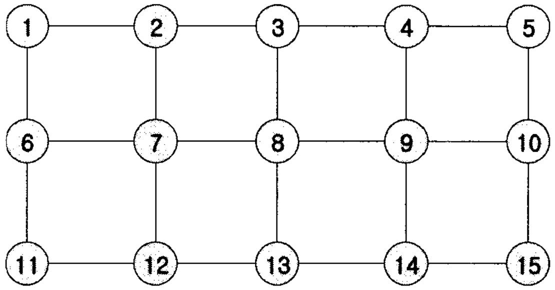

Fig. 3. A sensor network in 5×3 grid

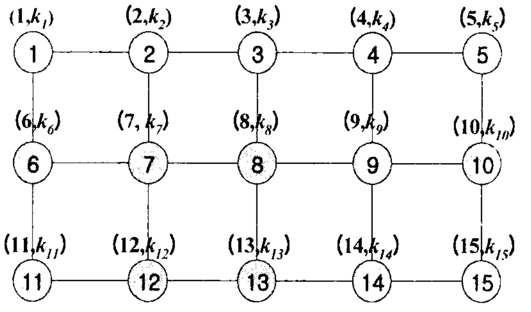

Fig. 4. Every node has IDs with secret key

First, all the nodes are placed in the parentheses following its UID and a share assignment for the secret key *k*(this simulation doesn't consider public key), as in Fig. 4.

After the simulation, there are the differences of communication overhead in three methods of IDs assignments.

In case of the proactive IDs assignment, it broadcasts periodic HELLO message in every transmission. In addition, every node broadcast the periodic HELLO message to each other to assign IDs. Thus, the case causes very high communication overhead.

In case of the reactive IDs assignment, it broadcasts HELLO message in the end of the simulation to construct the neighbor table. However, the case keeps going on sending CHANGE message in order to avoid the ID conflict problem. In this case, communication overhead quite high.

Last, in case of the hybrid IDs assignment, communication overhead is lower than the other two schemes. Because it targets only a few cluster head to assign IDs in each zone.

In result, the proposed scheme successfully reduces the optimization complexity, and solves traffic problem that exists in sensor networks.

The number of packets received at each node after doing each phase of procesures is shown in Fig. 5.

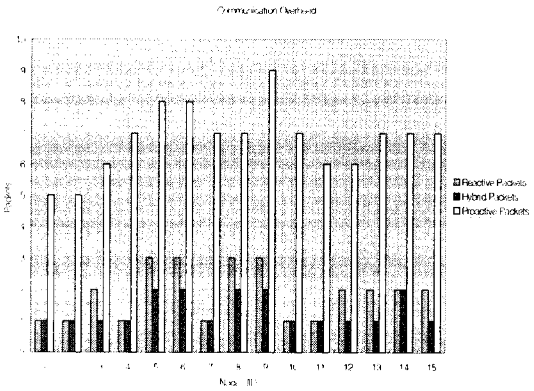

Fig. 5. The number of packets received at each node for 2 broadcasts

The table shows the advantages , the disadvantages, and characteristic among those three schemes in Table 1.

Table 1. The characteristics of three IDs assignments

schemes characteristics	Proactive IDs assignment	Reactive IDs assignment	Hybrid IDs assignment
Communication overhead	very high	high	low
Security	bad	bad	good
Optimization comlexity	much	much	a little
Energy consumption	high	high	low

5. Conclusions

This paper presents a hybrid IDs assignment scheme which combines a reactive IDs assignment scheme with a proactive IDs assignment scheme. The proposed hybrid scheme is considered a question in all of aspect. Specially, combined with a directed diffusion communication paradigm, the hybrid scheme considers communication overhead, and security in

USN.

For communication overhead, the scheme introduces a reactive IDs assignment scheme[9] which defers ID conflict resolution until data communicatons are initiated. And it communicates only a few cluster head to assign IDs in each zone. For security, it considers Byzantine Agreement Protocol of Proactive AVSS[13] as a proactive IDs assignment scheme.

This protocol for transmission state is not suitable to the nodes of a sensor network because any node in sensor networks can be a source node. Therefore, the proposed scheme introduces the zone-based self-organized clustering with unique IDs.

This protocol can communicate securely even if there are the corrupted parties included malicious, bogus nodes. Thus, proactive IDs assignment scheme has solved the problem[10] of repairing the network from the effect of an aberrant node.

Future work is to establish efficient key managements of the global zone in the sensor networks.

References

[1] K. Sohrabi, J. Gao, V. Ailawadhi, and G. Pottie, "Protocols for Self-Organization of a Wirless Sensor Network", IEEE Personal Comm. Magzine, vol. 7, no. 5, pp.16-27, Oct. 2000.

[2] P. Saffo, "Sensors:The Next Wave of Innovation", Comm. ACM, vol. 40, no.2, pp.92-97, Feb. 1997.

[3] G. Pottie, "Hierarchical Information Processing in Distributed Sensor Networks", Proc. Int. Symp. Information Theory Conf.(ISIT'98), pp.163, Aug. 1998.

[4] H. Zhou, Matt W. Mutka, and Lionel M. Ni, "Reactive ID Assignment for Sensor Networks", MASS 2005.

[5] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", in Proceedings of MobiCom 2000, Boston, MA, Aug. 2000.

[6] K. Weniger and M. Zitterbart, "IPv6 autoconfiguration in large scale mobile ad-hoc networks", In Proceedings of European Wireless 2002, Florence, Italy, Feb. 2002.

[7] M. Mohsin and R. Prakash, "IP address assignment in a mobile ad hoc network", In Proceedings of MILCOM 2002, Anaheim, CA, Oct. 2002.

[8] H. Zhou, L. M. Ni, and M. W. Mutka, "Prophet address allocation for large scale MANETs", Ad Hoc Networks Journal, Vol. 1, Issue 4, pp. 423-434, Nov. 2003.

[9] H. Zhou, Matt W. Mutka, and Lionel M. Ni, "Reactive ID Assignment for Wireless Sensor Networks", International Journal of Wireless Information Networks, Vol.13, No. 4, pp.317-328, Oct. 2006.

[10] Security for Sensor Networks, http://www.csee.umbc.edu/cadip/2002Symposium/sens or-ids.pdf, Oct. 2002.

[11] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem", ACM Transactions on programming languages and systems, 4(2), pp.382-401, 1982.

[12] D. Dolev, C. Dwork, O. Waatz, and M. Yung, "Perfectly Secure Message Transmission", Journal of the ACM, 40(1), pp.17-47, Jan. 1993.

[13] Soon Hwa Sung, Eun Bae Kong, "Byzantine Agreement with Threshold Cryptography in Unknown Networks", SAM'04, pp.68-74, Jun. 21-24, 2004.

[14] E. Ould-Ahmed-Vall, D. M. Blough, B.S.Heck and G.F. Riley, "Distributed Unique Global ID

Assignment for Sensor Networks", In Proceedings of IEEE International Conference on Mobile Ad hoc and Sensor Systems, Washington DC, Nov. 2005.

[15] M. Ali and Z.A.Uzmi, "An energy efficient node address naming scheme for wireless sensor networks", in Proceedings of the International Networking and Communications Conference(INCC), 2004.

[16] W. B. Heinzelman, J. W. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks", in Proceedings of MOBICOM, 1999.

[17] Soonhwa Sung, "Zone-Based Self-Organized Clustering with Byzantine Agreement in MANET", Journal of Communications and Networks(JCN), Volume 10, Number 2, ISSN1229-2370, June 2008.

[18] Network Simulator, http://www.isi.edu/nsnam/ns, July 2006.

◐ 저자소개 ◑

성 순 화(Soonhwa Sung)

1983년 경북대학교 전자학과(전산) 졸업(학사)
2000년 한남대학교 대학원 컴퓨터공학과 졸업(석사)
2005년 충남대학교 대학원 컴퓨터공학과 졸업(박사)
2001년 ~ 2004년 대덕대학 겸임교수
2002년 ~ 2005년 충남대학교 시간강사
2006 ~ 현재 충남대학교 전기정보통신공학부 BK교수
관심분야 : 정보 보안, 유비쿼터스 컴퓨팅 보안, 인터넷 보안, 미래 인터넷을 위한 사용자 인증 시스템 etc.
E-mail : shsung@cnu.ac.kr