Journal of Computer Science 8 (10): 1711-1717, 2012
ISSN 1549-3636

Routing Based Data Security in Mobile Ad Hoc Network Using Group Key Management

Mohanraj, E. and K. Duraiswamy
Department of Computer Science and Engineering,
K.S. Rangasamy College of Technology, Tiruchengode, Tamil Nadu, India

Abstract: Problem statement: A mobile ad-hoc network (MANET) is a self-organizing system of mobile devices followed an infrastructure less framework associated by wireless links. In MANET, there is a possibility of packet data to get lost or hacked by an attacker. So, to improve a secure communication over MANET from attackers, several techniques have been developed. The previous work developed to provide an efficient communication in Mobile Ad Hoc Networks by adapting an optimization technique of Ant Colony Optimization with Fairness Index and provides an authentication services to data. But the drawback is that there is a possible for the authorized user in MANET can access the unauthorized data and the authentication services for data are used only to defend communication on clear mediums in wireless networks. **Approach:** To improve the secure data communication in MANET, in this work we present a routing based data security by using multicast group key management. The proposed work routing based data security describes the process of secure the data while on communication through a specified route using group key management. **Results:** The group key management efficiently manages the data communication in MANET using key derivative function. A Key Derivation Function (or KDF) used to derive a secret key formed by a secure group on MANET. **Conclusion:** An experimental evaluation show that the proposed routing based data security by using multicast group key management outperforms well in terms of key maintenance, communication overhead, security.

Key words: MANET, data security, routing, group key management, key derivative function

INTRODUCTION

MANET: A Mobile Ad-Hoc Network (MANET) is a self-constructing infrastructure fewer networks linked for a communication using wireless links. Each and every node in a MANET is free to progress independently in some track and will consequently modify its links to other devices regularly. Each node should promote traffic not linked to its individual use and hence be a router. The most important confront in building a MANET is furnishing each node to constantly preserve the information vital to correctly route traffic. Such type of networks may function by them or may be linked to the larger Internet. MANETs generally has a routable networking atmosphere.

Data security: In MANET, Data Security means defending a database from negative forces and the unnecessary events of unauthorized users. Several technologies are presented in generic for data security. They are disk encryption, Hardware based mechanism for protecting data, Backups, Data masking. Disk encryption describes the process of encryption tools that encrypts data on a hard disk drive. Hardware based security provides a substitute to computer security. Security tokens are used for a data authentication purpose. Backups are used to guarantee data which is vanished can be improved. The method of masking precise data inside a database to guarantee that data security is sustained and perceptive information is uncovered to unauthorized people is called as data masking.

Characteristics of MANETs: To discover and preserve routes between nodes in an active topology with probably uni-directional links, using lowest amount of resources. Normally the main characteristic of MANETs is dynamic topology. The routes are formed with a group of nodes and due to mobility in nature for MANET, links are broken (Fig. 1).

Corresponding Author: Mohanraj, E., Department of Computer Science and Engineering, K.S. Rangasamy College of Technology, Tiruchengode, Tamil Nadu, India

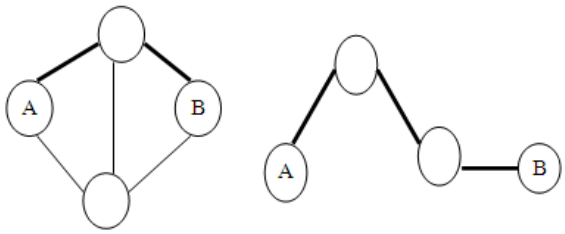

Fig. 1: Dynamic topology of MANET

To improve the data communication in MANET which is dynamic topology in nature has a possibility to access the data even by authorized user. So, to protect the packet data which is to be passed in MANET, keying mechanism is used. The Group key management is done based on the authorized users' using key derivative function for managing the secret keys among the users in the MANET environment. None other technique describes the process of protecting the packet data while on router from source to destination.

Related work: In MANET, a communication is done based on the nodes present in MANET. Since MANET is dynamic topology in nature, the node mobility changes at every time. So, the communication in MANET is unsecured one. To make MANET as secure (Lim *et al*., 2009) proposed new methods for communication with nodes, developed a technique to model the result of authentication on security. Since MANET used under dynamic topology in nature, the mobility of node are handled (Melodia *et al*., 2009) by using the wireless sensor and actor networks. A coordination and communication problems in WSANs with mobile actors are studied. Actors broadcast location updates limiting their scope based on Voronoi diagrams, while sensors predict the movement of actors based on Kalman filtering of previously received updates.

For a secure data collection in MANET, (Shu *et al*., 2010) presented a randomized dispersive routes for a wireless sensor networks. It developed mechanisms that produce randomized multipath routes. To provide a good QoS (Quality of Service) in MANET, (Burmester and Medeiros, 2009) developed a QoS self optimization in MANET for a secure communication in a wireless ad-hoc network. A single-hop transmits system with a straight link between the source and the destination is measured by the concept of signal space diversity (Ahmadzadeh *et al*., 2010). To provide a QoS service efficiently in MANET, (Zhang *et al*., 2012) presented a challenges and solutions for tradeoff between query processing in MANET by providing good services for a secure data communication.

To distributive a group mobile nodes with similar mobility pattern into a cluster, (Dang and Wu, 2010) proposed a cluster-based routing protocol for Delay-Tolerant Mobile Networks (DTMNs). For an efficient and dynamic routing, (Ni *et al*., 2010) presented a topology inference from end-to-end measurements. In (Amine *et al*., 2009) presented a substantiation method for inter domain wandering for 3G/WLAN systems. In QoS, path selection depends on path recognitions where higher tribute paths are privileged. CBR also observed flow blocking probabilities for every path to utilize in outlook paths (Roy *et al*., 2012). QBR ensured a path and renovated flow values into standard path traits. QBR proceeds flourishing flow and penalizes flow error like CBR (Llewellyn *et al*., 2011).

MATERIALS AND METHODS

The proposed routing based data security is efficiently designed for a secure communication in MANET using Group Key Management services. The proposed RBDS (routing based data security) carries out by three operations. The first phase describes the process of identifying the route to pass a packet data from source to destination. The second phase describes the keying mechanism to secure the packet data. The third phase describes how the packet data has been secured from an authorized attacker. The architecture diagram for the proposed RBDS using GKM (Group Key Management) is shown in Fig. 2.

Route discovery: When source node s contains data to promote to a destination d, it investigates its routing table for next best hop to attain destination. Node s begins a route request message ROUTEREQ_ ANT via all its neighbors. While traveling to destination, ROUTEREQ_ANT verifies available ability of every link, character of hops it has seen. If obtainable ability of link seen is lesser than that of in ROUTEREQ_ANT message, the available bandwidth area in ROUTEREQ_ANT message is updated by newly seen link's capacity. This will construct request message to take minimum available bandwidth of a link along the path it has passed. Finally, when RROUTEREQ_ANT arrives at the destination, it will be transformed as route reply message called ROUTEREP_ANT. The ROUTEREP_ANT will obtain similar path of corresponding ROUTEREQ_ANT, but in repeal direction. For this, ROUTEREP_ANT replicates and changes stack of nodes seen by ROUTEREQ_ANT as stack of nodes to be seen.

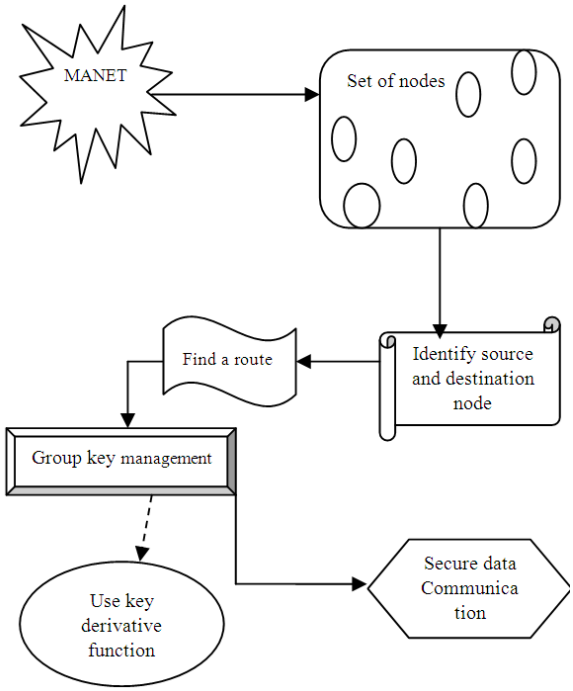

Fig. 2: Architecture diagram of RBDS using GKM

At every node from ROUTEREP_ANT's preliminary point, stack is popped to notice next hop to forward ROUTEREP_ANT. At intermediate nodes and at source s, message coming along with ROUTEREP_ANT such as delay, bandwidth and hop count are used to estimate path preference probability to contact destination. Source node s updates path preference to destination d via its whole neighbors given, it has received ROUTEREP_ANT via these neighbors. The neighbor node which contributes a superior path preference over all neighbors of node s is chosen as finest next hop to attain destination d. After routing table is updated with best next hop for preferred destination d, data transmission begins via that finest next hop.

The mathematical model is to find a path from source to destination through a neighbor with maximum path preference probability. Path preference probability from source s to destination d through s's neighbor x is calculated as Eq. 1:

$$p_{sxd} = \frac{[T_{sx}]^t[D_{sxd}]^{de}[H_{sxd}]^h[BW_{sxd}]^b}{\sum_{me N_s}[T_{sx}]^t[D_{sxd}]^{de}[H_{sxd}]^h[BW_{sxd}]^b} \quad (1)$$

where Ns is a set of neighbor nodes of s, T_{sx} relative weight of pheromone trail on link (s, x), D_{sxd} is relative metric for delay on the path from s to d through x, H_{sxd} Relative metric for number of nodes on the path from s to d through x, BW_{sxd} available bandwidth of the path from s to d through x, t, de, h and b tunable parameters which represent the importance of pheromone decay, delay, number of hops and available bandwidth on the path from s to d through x.

Group key management for data security: After identifying the route from source to destination, the keying mechanism is applied to the packet data to secure the data while routing from an attacker. Even though the authorized persons are accessing the data, it is possible for then to acts as an attacker to derive the data which is not authorized to them.

A group key management (GKM) chains confined statement among members of a secure group. A secure group is a major group of members, who might be senders, receivers, or both to other members of the group. Group relationship might change over time. A group key management protocol facilitates to guarantee that only members of a secure group can grow access to group data and can validate group data. The objective of a group key management protocol is to offer genuine group members with the up-to-date cryptographic state they require for confidentiality and authentication. The overall design of the Group Key management data security model is shown in Fig. 3.

Each group member, i.e., sender or receiver, used the registration process to get authoritative and genuine access to a scrupulous Group, its policies and its keys. Key encryption keys (KEKs) and the traffic encryption keys (TEKs) are the two types of group keys. The KEK could be a sole key that shields the rekey message, normally enclosing a new Rekey SA (containing a KEK) and/or Data SA (containing a TPK/TEK). The data security used TPKs to shield streams, files, or other data sent and received by the user.

The Group Key Management is done based on the nodes present in MANET. For an instance, if the average number of nodes in the MANET is $n=\lambda_p O$, where λ_p specifies the node density of the randomly distributed nodes and O describes the operational area of MANET wireless medium. The random distribution of nodes is done based on homogeneous spatial Poisson process. There is a chance for the nodes to be joined or leaved at any point of time. Therefore, the probability of the node P(g) is in any group is Eq. 2:

$$P(g) - \lambda/(\lambda+\mu) \quad (2)$$

And the probability P(g') that it is not in any group is Eq. 3:

$$P(g') - \mu/(\lambda+\mu) \quad (3)$$

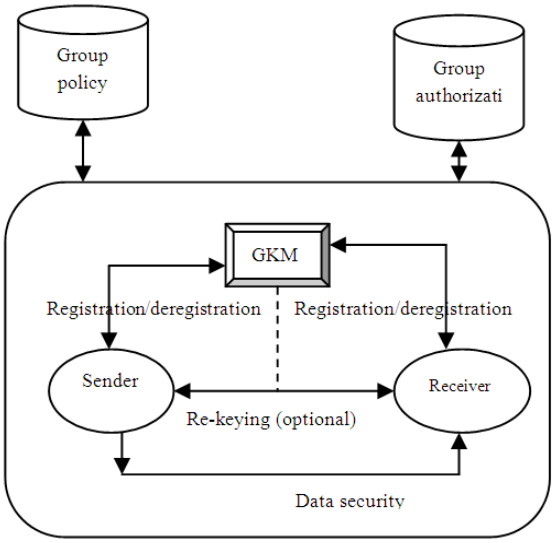

Fig. 3: Group Key management data security model

The main characteristics of GKM for data security are as follows:

- It efficiently presents privacy and substantiation, replay protection and DoS protection from attacks
- An efficient rekeying once transforms in group membership
- A consistent deliverance of rekey messages
- A high throughput and low latency,

After assigning the group key for all groups in MANET, if we want to transmit a message from one group to other group, then the source group sends the data with a key i.e., no one can access the data without deriving a key. So, the destination group can access the data only by deriving a key using key derivative function.

Algorithm for joining the group:

JOIN (A, B = b_i) {i = 0,1,2,…n} B-existing member in group
Step1: Begin
Step2: A = a_i where {i=0, 1, 2…n}
Step3: m = 1
Step4: While (m< = length (A))
Step 5: Begin
Step6: Assign Mem_id for incoming group/member
Step7: Associate the key K with A
Step9: Send key from k' to X using Mem_id
Step10: Secure the data using k' and Mem_id
Step11: Join the group
Step12: End
Step13: End

To maintain all the members of the group, it is necessary to monitor the members of the groups that who is joining and who is leaving the group. Key associations are considered to entrust the charge of key distribution consistently with all the senders. The above algorithm is used for joining the group and assigning the key to the new member for a secure communication and also to check the authorization.

Algorithm for leaving the group:

LEAVE (A)
i = 1
Step1: Begin
Step2: Identify the neighbor of B (existing member)
Step3: Remove the member/ Mem_id of A from the group
Step4: Change the secret key
Step5: Initiates rekeying process
Step6: While (i< = length (B))
Step7: Begin
Step8: Assign new key K to all members in a group
Step9: Assign Mem_id to all members
Step10: End
Step11: End

The above algorithm is used for leaving the group. If the member is decided leaving the group, then the Mem-id and secret key of the group changes. So, the group will start the rekeying process and assign a new key to every member in the group for a secure communication.

Key derivative function: If a source node sends a packet data to destination with a secret key, then the destination node in another group can only access the data only by identifying a key. A key can be identified and derived using key derivative function. Key derivation functions are used to obtain keys from secret passwords or passphrases, which classically do not have the preferred properties to be used openly as cryptographic keys. The key derivation function protects the data from attack or dictionary attack. The key derivative function may be expressed as Eq. 4:

$$KD = KDF (k, R, I) \quad (4)$$

Where:
KD = The derived key
KDF = The key derivation function,

K = The original key or password,
R = A random number which acts as cryptographic salt and I refers to the number of iterations of a sub-function

The derived key is used as a substitute of the unique key or password since the key to the system is used. The values of the salt and the number of iterations are gathered with the hashed password or sent as plaintext with a packet data.

All members in the multicast group can figure the root key by deriving with the given keys. A member in a group wants to send a data, first encrypts it using the root key and sends the data to destination via multicast channels. Other members in the same group can decrypt the data without any advanced key interactions.

RESULTS

The proposed Group Key Management is efficiently designed for a routing based data security process to provide a secure data communication in MANET. The proposed RBDS using GKM is implemented in NS-2 simulator. The simulations are carried to assess the performance of the proposed RBDS using GKM with dissimilar applications for a secure data communications in MANET. The radio model is based on the viable hardware with a wireless transmission range of 270 meters and channel capacity of 3Mbps. Each simulation runs for 270 seconds and the results are compared with an existing Integrated Security and QoS Routing and Data Communication Framework (ISQRDC) which is designed only for an authentication purpose. The proposed RBDS using GKM infrastructure framework is designed in (Fig. 2). The proposed RBDS for a secure data communication carried three types of operations {route discovery, GKM, RBDS using GKM…..}. Operations can be assigned to different services of nodes in the infrastructure framework. The performance of the proposed RBDS using GKM is evaluated by the following metrics routing overhead, throughput, security group.

Routing overhead: Since, MANET is dynamic topology in nature, there is a chance of a member in a group moves from its group. So while applying GKM to that group, the area keys of the member could be changed. At the time of movement, rekeying overhead arise. Larger rekeying overhead arises, when member leaves domain of the MANET. In the proposed RBDS using GKM, rekeying overhead is less compared to an existing Integrated Security and QoS Routing and Data Communication Framework (ISQRDC). The above table (Table 1) describes the routing overhead arise while the members in the gropu leaves the domain in MANET. The table compares the routing overhead of the proposed RBDS using GKM with an existing ISQRDC.

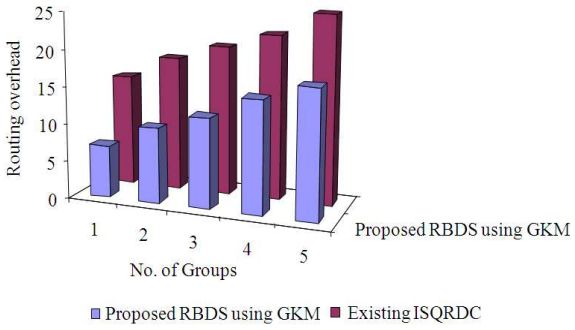

Fig. 4: No. of groups vs. Routing overhead

Table 1: No. of groups Vs. Rekeying overhead

	Routing overhead	
No. of groups	Proposed RBDS using GKM	Existing ISQRDC
1	7	15
2	10	18
3	12	20
4	15	22
5	17	25

Table 2: No. of messages in groups Vs. Throughput

	Throughput (%)	
No. of messages in groups	Proposed RBDS using GKM	Existing ISQRDC
10	25	10
20	34	19
30	40	25
40	45	32
50	50	35

Fig. 4 describes the process of routing overhead arises in secure groups formed in MANET using GKM. Sincer the group has been formed using GKM in MANET, the routing overhead chances are less in the proposed RBDS using GKM. In the proposed RBDS using GKM, the packet data has been transferred using data security process so, there is a less chance in routing overhead. The performance graph of the proposed RBDS using GKM in routing overhead is shown in the Fig. 4. The variance in the routing overhead for routing the packet data from source to destination would be 15-25% low in the proposed RBDS using GKM compared to an existing ISQRDC.

Throughput: It is defined as the average rate of successful message delivery over a communication channel from one group to another group in MANET. The throughput is generally calculated in bits per second (bit/s or bps) and sometimes in data packets per second or data packets per time slot. The above table (Table 2) describes the throughput for the successful delivery of messages over MANET. The table compares the throughput of the proposed RBDS using GKM with an existing ISQRDC.

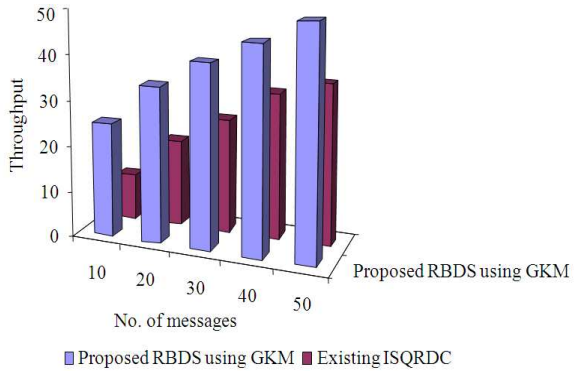

Fig. 5: No. of messages in groups vs. Throughput

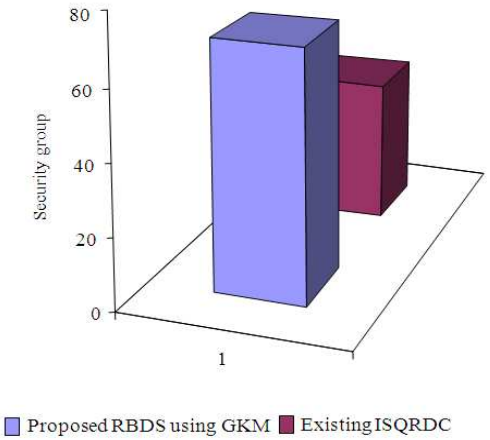

Fig. 6: Security level of group in MANET

Table 3: Security level of group in MANET

	Security level of group in MANET (%)	
Method	Proposed RBDS using GKM	Existing ISQRDC
	70	40

Figure 5 describes the throughput for successful delivery of messages in MANET using GKM. Sincer the group has been formed as secure using GKM in MANET, the deliver rate of packet data is high in the proposed RBDS using GKM. In the proposed RBDS using GKM, the packet data has been transferred using data security and the routing discovery process is made at first. The performance graph of the proposed RBDS using GKM in throughput is shown in the Fig. 4. The variance in the throughput for delivery of packet data from source to destination would be 50% high in the proposed RBDS using GKM compared to an existing ISQRDC.

Security Group is termed as members of group alone can access only their authorized data and none other group in MANET can access those data which is authorized to that group alone. The security level of the group is high. The above table (Table 3) describes the security level of group for data communication in MANET. The table compares the security level of the proposed RBDS using GKM with an existing ISQRDC.

Figure 6 describes the security level of the group formed by using GKM formed in MANET. Sincer the group has been formed using GKM in MANET; the level of security is high in the proposed RBDS using GKM. In the proposed RBDS using GKM, the packet data has been transferred using keying mechanism, there is a less chance for accessing the data to attacker/ unauthorized user. The performance graph of the proposed RBDS using GKM in security level is shown in the Fig. 6. The variance in the security level of the group for routing the packet data from source to destination with a keyimg mechanism would be 50-70% high in the proposed RBDS using GKM compared to an existing ISQRDC.

DISCUSSION

In this study, we have seen that the proposed Routing Based Data security is efficiently designed using Group Key management for an effective secure communication by securing the data on routing. It secures the dat which is being transmitted in MANET for service performance to other systems written in NS-2 simulator. We run independent tests with growing number of nodes in MANET and constant number of packet data sent by source to destination secure group. The below table and graph describes the performance of the proposed RBDS using GKM.

Finally, it is being observed that the proposed RBDS using GKM has efficiently desgined for an effective communication in MANET using Group Key management bt creating a key for each group and using key, security groups could communicate in a a secure manner for transmitting the packet data.

CONCLUSION

In this study, we have presented an RBDS (Routing Based Data Security) framework, to enhance the security in mobile ad hoc networks for an efficient communication. In RBDS, Security and an effective data communication considered together due to overheads initiated by an attacker by attacking or accessing the unauthorized data in ad hoc networks. The proposed RBDS have developed based on Group

Key Management. Using GKM, security groups have been formed and the communication is done based on keying mechanism. Group Key management is introduced for improved secure communication guided routing to nodes in MANET and for data communication security on receiving the data or sending the data to and from other mobile nodes. Experimental simulations are carried out to evaluate the performance of the proposed frame work RBDS using GKM in terms of throughput, security level, routing overhead. Compared to an existing ISQRDC which is designed only for authentication purpose, here in the proposed work, it takes care over a secure data communication in MANET.

REFERENCES

Burmester, M. and B.D. Medeiros, 2009. On the security of route discovery in MANETs. IEEE Trans. Mobile Comput., 8: 1180-1188. DOI: 10.1109/TMC.2009.13

Dang, H. and H. Wu, 2010. Clustering and Cluster-Based Routing Protocol for Delay-Tolerant Mobile Networks. IEEE Trans. Wireless Communi., 9: 1874-1881. DOI: 10.1109/TWC.2010.06.081216

Ni, J., H. Xie, S. Tatikonda and Y.R. Yang, 2010. Efficient and dynamic routing topology inference from end-to-end measurements. IEEE/ACM Trans. Networking, 18: 123- 135. DOI: 10.1109/TNET.2009.2022538

Amine, K., K. EI Yassini and D. EI Oouadghiri, 2009. Multicriteria formulation for the quality of service in ad hoc networks. Proceedings of the International Conference on Multimedia Computing and Systems, Apr. 2-4, IEEE Xplore Press, Ouarzazate, pp: 395-399. DOI: 10.1109/MMCS.2009.5256664

Llewellyn, L.C., K.M. Hopkinson and S.R. Graham, 2011. Distributed fault-tolerant quality of wireless networks. IEEE Trans. Mobile Comput., 10: 175-190. DOI: 10.1109/TMC.2010.148

Roy, S., M. Conti, S. Setia and S. Jajodia, 2012. Secure data aggregation in wireless sensor networks. IEEE Trans. Inform. Forens. Secu., 7: 1040-1052. DOI: 10.1109/TIFS.2012.2189568

Ahmadzadeh, S.A., S.A. Motahari and A.K. Khandani, 2010. Signal Space Cooperative Communication. IEEE Trans. Wireless Communi., 9: 1266-1271. DOI: 10.1109/TWC.2010.04.090059

Lim, S., C. Yu and C.R. Das, 2009. RandomCast: An energy-efficient communication scheme for mobile ad hoc networks. IEEE Trans. Mobile Comput., 8: 1039-1051. DOI: 10.1109/TMC.2008.178

Shu, T., M. Krunz and S. Liu, 2010. Secure data collection in wireless sensor networks using randomized dispersive routes. IEEE Trans. Mobile Comput., 9: 941-954. DOI: 10.1109/TMC.2010.36

Melodia, T., D. Pompili and I.F. Akyildiz, 2009. Handling mobility in wireless sensor and actor networks. IEEE Trans. Mobile Comput., 9: 160-173. DOI: 10.1109/TMC.2009.102

Zhang, Y., L. Yin, J. Zhao and G. Cao, 2012. Balancing the Trade-offs between query delay and data availability in MANETs. IEEE Trans. Parall. Distributed Syst., 23: 643-650. DOI: 10.1109/TPDS.2011.222