A Key Exchange Approach for Proficient and Secure Routing in Mobile Adhoc Networks

https://doi.org/10.3991/ijim.v11i4.6440

L. Raghavendar Raju
Matrusri Engineering College, Hyderabad, India
lraghavenderraju@gmail.com

C. R. K. Reddy
Chaitanya Bharathi Institute of Technology, Hyderabad, India
crkreddy@cbit.ac.in

Abstract—Mobile ad hoc networks (MANETs) are a collection of wireless mobile devices with restricted broadcast range and resources. Communication is achieved by relaying data along appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes is a major task, both from efficiency and security point of view. This paper presents a proficient and secure routing, based on asymmetric authentication using key exchange approach (KEA). The proposed mechanism ensures secure routing and quality of service in MANETs and minimizes the network overhead. The KEA mechanism can be effectively used to develop a new routing protocol for Mobile Adhoc Networks which will provide maximum security against all kinds of attacks. In this paper, KEA is compared with other secure routing protocols like EEACK, AODV, and ARIADANE, to evaluate the efficiency of KEA in Ad Hoc Networks. The empirical results show that there is an increase of 20% packet delivery ratio and a reduction of 10% routing overhead.

Keywords–Wireless network, Security, Routing, Key exchange, Asymmetric Authentication, MANET

1 Introduction

The exponential growth in the development and acceptance of mobile communications in recent years is especially observed in the fields of wireless local area networks, mobile systems, and ubiquitous computing. This growth is mainly due to the mobility offered to users, providing access to information anywhere, user friendliness, and easy deployment [7]. Furthermore, the scalability and flexibility of mobile communications increase users' productivity and efficiency. Dynamic ad hoc networks are formed by a set of mobile terminals placed in a close location that communicate with each other, sharing resources, services or computing time during a limited period of time and in a limited space, following human interaction pattern [2][3][4].

Dynamics adhoc networks require well defined, efficient and user-friendly security mechanisms. Tasks to be performed include: user identification, their authorization, address assignment, name service, operation, and safety. Generally, wireless networks with infrastructure use Certificate Authority (CA) servers to manage node authentication and trust [5][9][11][19]. Although these systems have been used in wireless ad hoc and sensor networks [13], they are not practical because a CA node has to be online (or is an external node) all the time. Moreover, CA node must have higher computing capacity**.**

Security should be based on the required confidentiality, node cooperation, anonymity, and privacy. Exchanging photos between friends requires less security than exchanging confidential documents between enterprise managers. Moreover, all nodes may not be able to execute routing and/or security protocols. Energy constraints, node variability, error rate, and bandwidth limitations mandate the design and use of adaptive routing and security mechanisms, for any type of devices and scenarios [6].

Dynamic networks with flexible memberships, group signatures, and distributed signatures are difficult to manage [15]. To achieve a reliable communication and node authorization in mobile ad hoc networks, key exchange approach (KEA) for node authorization and user authentication are needed. We propose a secure and proficient secure routing approach using key exchange approach.

The rest of the paper is organized as follows: Section 2 presents the related work on dynamic networks and shows the most well-known security mechanisms that can be applied to them. The proposed secure key exchange approach is described in Section 3. Section 4 presents the experiment evaluation mechanism and performance analysis of our proposal. Finally, Section 5 presents the conclusion and future work.

2 Related Works

The related literature shows several security methods such as pre-distribution key algorithms [15], symmetric and asymmetric algorithms, intermediate node-based methods [8], and hybrid methods [14]. But these methods are not enough for dynamic networks because they need an initial configuration (i.e., network configuration) or external authorities (for example, central certification authorities).

In [20], Latvakoski et al. explain a communication architecture concept for dynamic systems, integrating application-level dynamic group communication, and ad hoc networking together. A set of methods to enable plug and play, addressing and mobility, peer to peer connectivity and the use of services are also provided.

Liu et al. [18] show how networked nodes can autonomously support and cooperate with each other in a peer-to-peer (P2P) manner to quickly discover and self-configure any services available on the disaster area and deliver a real-time capability by self-organizing themselves in dynamic groups to provide higher flexibility and adaptability for disaster monitoring and relief.

K. Liu et al. [16] proposed TWOACK is one of the most important approaches for intrusion detection in MANETs. TWOACK detects misbehaving links by acknowl-

edging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR).

Feeney et al. [21] presented Spontnet, a prototype implementation of a simple ad hoc network configuration utility based on the main ideas of dynamic networks. Spontnet allows users (using face-to-face authentication and short-range link with easily identifiable endpoints) to distribute a group session key without previous shared context and to establish shared namespace. Two applications, a simple web server and a shared whiteboard, are provided as examples of collaborative applications. They use IPSec protocol (used for Virtual Private Networks), applied though internet. Spotnet therefore uses both wired and wireless links and corresponding protocols.

Ariadne [17] is an on-demand routing algorithm based on the Dynamic Source Routing (DSR) protocol [2]. There are several variants of Ariadne, depending on which mode of authentication is used to protect route requests: one uses digital signatures, one TESLA [22], and one uses MACs. The MAC version has an optimized variant that uses iterated MAC computations instead of several independent MACs. In addition to being more efficient, the iterated MAC version has superior security characteristics when compared to the no optimized version.

Elhadi M. S. et al., [1] proposed EAACK known as Enhanced Adaptive Acknowledgment for intrusion-detection system for MANETs. The work majorly targets the Packet-dropping attack which has always been a major threat to the security in MANETs. It puts in an effort to prevent the attackers from initiating forged acknowledgment attacks by incorporating digital signatures.

This paper presents a security protocol for routing purposes, based on key exchange as discussed in section-3. It presents three stages for secure routing as, Key acquisition, Neighbor discovery and secure key exchange routing in adhoc protocols for wireless.

3 Key Exchange Approach

In adhoc routing protocol nodes exchange information to their neighbourhood and construct a virtual network for data packet routing to their desired destination. Such information can be easily targeted by any malicious adversary who intentionally want to disrupt the functionality of the network. Attackers generally inject erroneous routing information externally to repeat previous routing messages, or modify the valid routing information and eventually bring the network down. Sometimes due to internal attacks, it causes severe damages as these nodes are not up to their initial commitments. Such nodes can also send erroneous information to modify the local view of the network. Usually it is very difficult to identify the internal attacker, since they already have some sort of credentials that everybody believes.

Our proposed targets are both, external and internal attacks which can exist in the network due to malicious nodes. It identifies these attacks based on the three security mechanisms as, Certificate Acquisition, Secure Route Discovery and Secure Data Routing. It uses Certificate Authority (CA) certificate to identify the internal attackers and use both symmetric and asymmetric cryptography for securing from external attackers. To prevent routing information from forged or tampered we use CA certificate for encrypting the messages.

3.1 Key Acquisition

Establishing security association between the mobile nodes is the most difficult part in ad hoc network. The difficulty is due to the nature of mobile ad hoc networks where predefined architecture for the security one cannot use. Most work related to security association and key distributions has not been addressed well in most of the previous secure routing protocols. One simple solution is described in [12] for the existence of security association between source and destination nodes. A group key exchange is described in [14] which is based on a strong sharing key, but this approach required a static group node and in dynamic network where the node joins and leaves very frequently. The group key should be updated in the process for all the nodes.

In [23][24] describes another security association process among the nodes which uses asymmetric cryptography where any node in the network can issue certificate for new nodes. This is a strong approach in sense of that it does not have any single point failure in the network. But it still can have vulnerability attacks as to authenticate a new node and issue a certificate which is risky if malicious nodes are already present in the network.

In KEA protocol, to have an initial security association among the node we also distribute the certificates. But these certificates are obtained from a trusted certified authority (CA), and it has to be loaded to each node I prior to join the network. This will be an offline process where each node by providing its identity to CA needs to obtain its certificate. In this approach if any node tries to posses an invalid certificate illegally can be identified and isolated easily.

The certificate issued by the *CA* for a node *N* consists of CA public key as CA_{pub_key}, node address as N_{add}, public key as N_{pub_key} and private key as N_{pvt_key}. The certificate is represented as,

$$C_N = Enc_{CA_{pkey}}(N_{add}, N_{pub\_key}, N_{pvt\_key}, CA_{pub\_key}).$$

We assume that all the valid nodes in the network obtain this certificate before joining the network. This process of acquiring certificate provides the basic identification to the node and prevents it from internal malicious nodes.

3.2 Secure Routing Process

Neighbor Discovery: The proposed KEA approach performs a neighbor discovery broadcasting a "*Hello*" message with in a restricted communication range. This mechanism reduces the power consumption required for distance broadcasting. Source node receives reply only from the nodes which are 1-hop away from the source. In exchange of "*Hello*" message it receives that node public key and a message signature for identification of the node authentication. The entire process is described in the Algorithm-1.

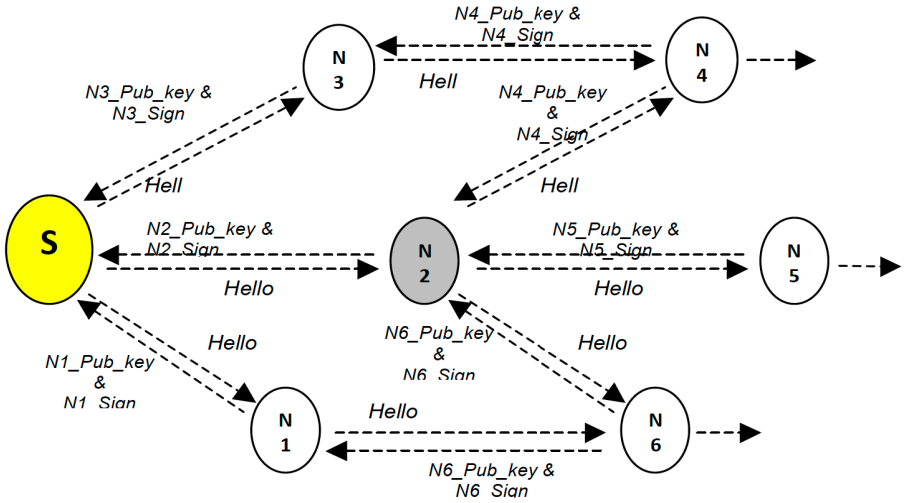

Fig. 1. Neighbor Discovery for Secure Routing

Algorithm 1: *Secure Neighbor Node Identification Mechanism*

Node *V* start Neighbor discovery Process → ***NeighborNodes (V)***

Method1: ***NeighborNodes (V)***
Assignment: *Msg* = "Hello".
V broadcast *Msg* in the network periodically to discover the secure neighbor nodes.
// *min_node – is the minimum number of neighbor node to be discover*
While *min_nodes* discovered
Receive Signed Message from Neighbor Nodes → N_{msg_sign}
If *path == 1-hop* **then**
V GenerateSignature(Msg) → V_{msg_sign}
If *validateSignature* (V_{m_sign} , N_{m_sign}) == *true* **then**
Add Node address to route table → *Route_Nodes[N,Ts]*
Add Node public key to node table → *Nodes_Key[N,* N_{pub_key}*]*
End If
End If
End While

This process is performed by the node periodically to update their route and node key table. It will also remove the node whose Timestamp *(Ts)* value is above the permitted time limit.

Secure Route Discovery: The KEA is capable of determining secure route by identifying each node message signature received during neighbor discovery of each individual node. The mechanism for secure node identification for authenticity and for the secure route discovery is described in Algorithm-2.

Algorithm 2: *Secure Route Discovery Mechanism*

Using the method ***NeighborNodes (V)*** each node maintains a set of nodes and its public keys in its *Route_Nodes* and *Nodes_key* Table.
To initiate a secure route Source Node ***S*** calls method → ***Init_RouteRequest(S)***

Method1: ***Init_RouteRequest(Node S)***
Assignment: *Msg* = "RREQ".
S Reads all the Nodes from its *Route_Node* table → $FH[\ ]$
S Reads each FH_i public key from its *Node_Key* table → FH_{pub_key}
S GenerateSignature (Msg, CA_{key}*)* → S_{msg_sign}
S Encrypt ([S_{msg_sign}, *Msg,* D_{add}, *Path[S])* using FH_{pub_key} → E_{msg}.
S sends E_{msg} to all its First Hops nodes it discovered during neighbor discovery process.
while FH_i is not destination node → D_{add} **do**
FH_i *Decrypt(*E_{msg}*)* using FH_{pvt_key} → [S_{m_sign} , *Msg* , D_{add}, *Path[S]]*
FH_i *GenerateSignature((Msg,* CA_{key}*)* → IS_{msg_sign}
If *validateSignature (*IS_{m_sign} , S_{m_sign}*) == true* **then**
If *Msg* == '*RREQ*' **then**
If FH_i == D_{add} **then**
Destination Node *D* → ***Do_RouteReply(***D_{add}***)***
Else
FH_i Append I_{add} to path data → *Path[S,* I_{add}*]*
FH_i *Encrypt ([*S_{msg_sign}, *Msg,* D_{add}, *Path[S,* I_{add}*])* using FH_{pub_key} → E_{msg}.
FH_i sends E_{msg} to all its First Hops nodes it discovered.
End if
End if
End if
End while

Method2: ***Do_RouteReply(D)***
Assignment: *Msg* = "RREP".
D Decrypt(E_{msg}*)* using D_{pvt_key} → [S_{m_sign} , *Msg* , D_{add}, *Path[S,* I_{add}*]]*
D GenerateSignature (Msg, CA_{key}*)* → D_{msg_sign}
D Encrypt ([D_{msg_sign}, *Msg,* S_{add}*])* using FH_{pub_key} → E_{msg}.
D sends E_{msg} to its First Hops nodes from which it receive in the request *Path [].*

On receiving the route reply from the destination, source node caches the path into its *Route_Table* for data routing.

On successful completion of secure route discovery, Source node sends data packet on the optimal route stored in the routing table based on the number of hop count.

Generally AODV [10] protocol maintains only one route from source to destination. In our scheme we also maintain the same, as multi-route discovery expense more overhead of storing more route information.

4 Empirical Evaluation

4.1 Simulation Methodologies

To better investigate the performance of KEA under different types of attacks, we propose two case settings to simulate different types of misbehaviors or attacks.

- *Case-1*: In this case, we simulated a basic packet dropping attack where malicious nodes simply drop all the packets that they receive. The objective of this case is to test the performance of the protocol against the existing secure protocols.
- *Case-2*: In this case it is designed to test protocol performances against false misbehavior report, where malicious nodes always drop the packets that they have received and send back a false misbehavior report whenever it is possible.

4.2 Simulation Setup

Experiment simulation is performed using Glomosim Simulator[x] to evaluate the performance KEA approach. It provides scalable and parameter driven environment for wireless protocol simulation. We compare the performance of KEA with AODV [10], ARIADANE [17] and EAACK (DSA) [1] for the evaluation. In order to perform the simulation we have taken the default wireless setting of Glomosim and with the setup parameters mentioned in Table-1. For each case, we ran each network scenario two times and calculated the average performance.

Table 1. Simulation Parameters

Configuration	Parameter Values
Simulation Area	1000m X 1000m
No. of Nodes	50
Mobility Speed	0 to 20 m/s
Source-Destination Pairs	15
Packet Size	512 bytes
CBR Rates	4 pkts/sec
Mobility	RWP
Pause Time (sec)	100
Malicious (%)	0, 10, 20, 30, 40, 50

In order to measure and compare the performances of our proposed approach, we continue to adopt the following two performance metrics.

A. Packet Delivery Ratio: Packet delivery ratio (PDR) defines the total number of data packets received against the total number of data packets sent by the source node.

B. Routing Overhead: Routing overhead calculation based on the total number of control packets is originated and forwarded by the protocols during the entire communication processes, such as RREQ, RREP, RERR and ACK.

4.3 Performance Evaluation

To provide a comparison performance analysis for a better insight of our simulation results, detailed simulation data are presented for Case -1 and Case-2 in Table 2. In case-1the malicious nodes drop all the packets that pass through it, whereas in case-2 we set all malicious nodes to send out false misbehavior report to the source node whenever it is possible. Figure-2 and 3 shows the simulation results of packet delivery ratio comparison for case -1 and 2. Figure-4 and 5 shows the Routing overhead comparison for case-1 and 2.

Table 2. Simulation data

Case-1: Packet Delivery Ratio (Absence of Malicious Node)					**Case-2: Packet Delivery Ratio (Presence of Malicious Node)**				
Malicious Node%	**KEA**	**AODV**	**ARIADANE**	**EEACK**	**Malicious Node%**	**KEA**	**AODV**	**ARIADANE**	**EEACK**
0	0.9982295	0.90066353	0.9376262	0.9782295	**0**	0.9982295	0.9006635	0.9376262	0.9782295
10	0.9898066	0.7115978	0.9064352	0.998066	**10**	0.9882547	0.6515978	0.8668695	0.998066
20	0.9607961	0.4443109 7	0.8017403	0.9407961	**20**	0.8970812	0.444311	0.6983455	0.9007961
30	0.8402318 2	0.3024656	0.7072595	0.7602318 2	**30**	0.8583679	0.3024656	0.5818386	0.7602318 2
40	0.8006182	0.2554980 6	0.5805658 6	0.6806182	**40**	0.6846594	0.2054981	0.4669054	0.6406182
50	0.6006047 2	0.2168307 2	0.5207909 82	0.5600604 72	**50**	0.5339198	0.1168307	0.2312847	0.5000604 72
Case-1 Routing Overhead Comparison(Absence of Malicious Node)					**Case-2 Routing Overhead Comparison(Presence of Malicious Node)**				
Malicious Node%	**KEA**	**AODV**	**ARIADANE**	**EEACK**	**Malicious Node%**	**KEA**	**AODV**	**ARIADANE**	**EEACK**
0	2390	3263	2635	2357	**0**	2390	3263	2635	2357
10	4961	5606	5246	3861	**10**	6061	10606	7246	5061
20	6435	6972	6009	5435	**20**	8036	12972	9009	6036
30	7061	12352	10645	6661	**30**	9546	16352	10645	8546
40	8508	21087	18064	8008	**40**	12841	22087	18864	9841
50	14252	28042	21390	12252	**50**	15966	27042	23390	10966

Figure-2 and 3 shows the case-1 and 2 packet delivery ratios for KEA and other approaches. In both the cases KEA shows high PDR and AODV shows low. KEA shows an improvisation of 20% in PDR in case-1 and 18% in case-2 in comparison to EEACK. The improvement is achieved due to the Secure Neighbor Node Identification Mechanism, which helps KEA a secure route to deliver high number packets.

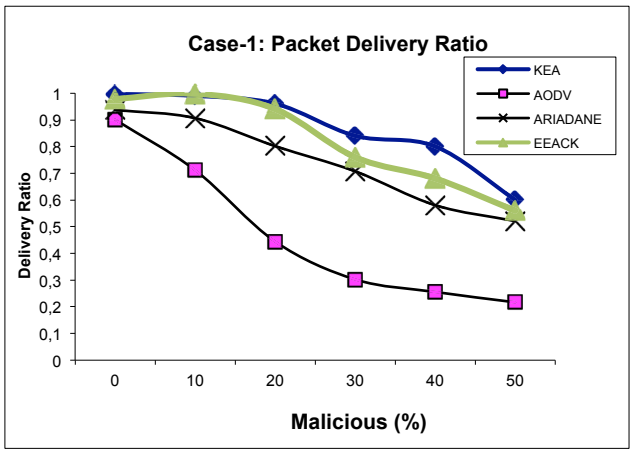

Fig. 2. Case-1 Packet Delivery Ratio Comparison

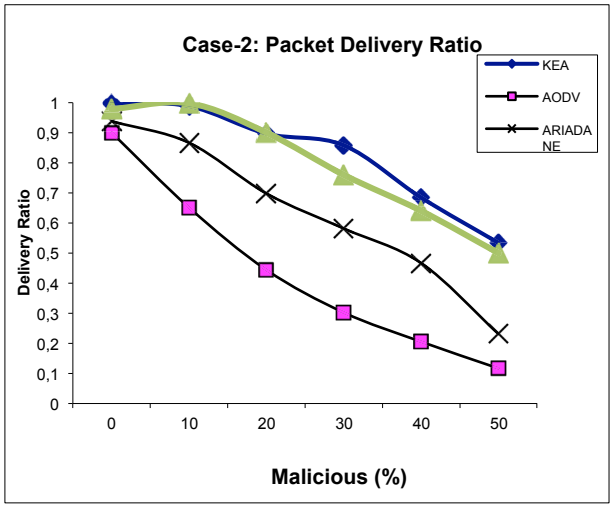

Fig. 3. Case-2 Packet Delivery Ratio Comparison

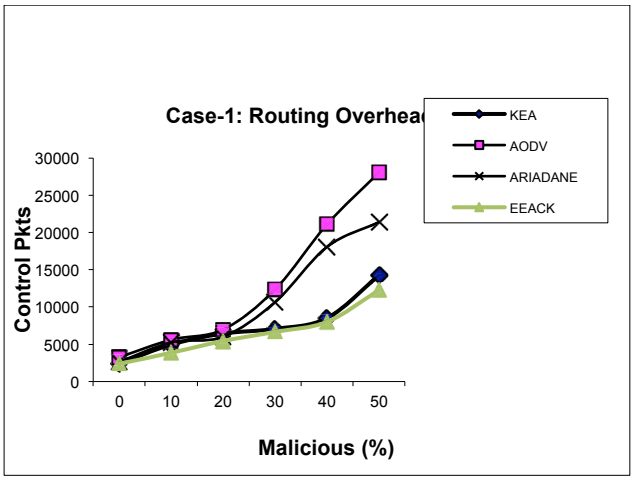

Fig. 4. Case-1 Routing Overhead Comparison

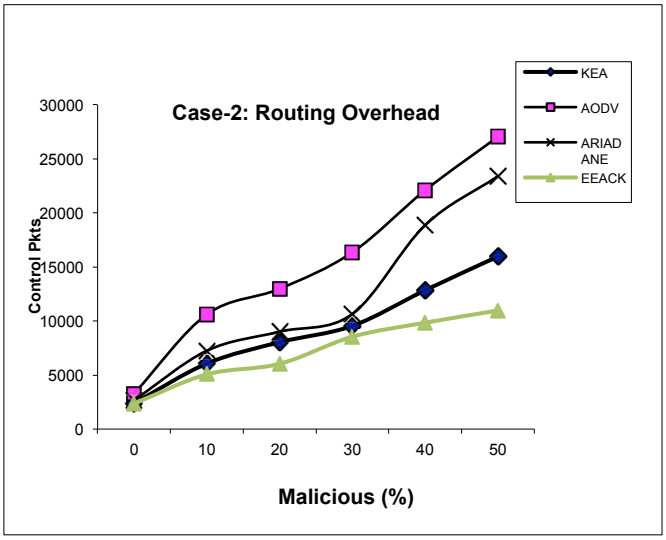

Fig. 5. Case-2 Routing Overhead Comparison

Figure-4 and 5 shows the case-1and 2 routing overhead comparison for KEA and other approaches. EEACK shows the low and AODV shows the highest overhead when compared to others with increasing malicious nodes. Whereas KEA shows 10% high overhead in comparison to EEACK as it is broadcasting a "*Hello*" message at the initial route discovery process to find the authenticate nodes.

5 Conclusion

Packet-dropping attack has always been a major threat to the security in MANETs. Due to overheads caused by implementing security in ad hoc networks, security and QoS must be considered together. We proposed a new Key Exchange Approach for proficient and secure routing protocol for mobile ad hoc networks. KEA authenticates the routing messages using digital signatures based on asymmetric cryptography. The KEA is capable of determining secure route. Security of the route is established through a message signature received during neighbor node discovery. The mechanism for secure node identification for authenticity and for the secure route discovery helps in improvising the throughput of PDR during communication. The empirical result shows a 20% high PDR with a bearable of 10% increase in routing overhead. In future work we optimize our approach to reduce more routing overhead compared to others.

6 References

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions On Industrial Electronics, Vol. 60, No. 3, March 2013 https://doi.org/10.1109/TIE.2012.2196010

[2] Adnan Nadeem, Member and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, Fourth Quarter 2013 https://doi.org/10.1109/SURV.2013.030713.00201

[3] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security", in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666. https://doi.org/10.1007/978-3-642-25769-8_92

[4] Dongxia Wang, Tim Muller, Yang Liu, and Jie Zhang, "Towards robust and effective trust management for security: A survey", In Proc. The 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2014.

[5] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET", in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387. https://doi.org/10.1007/978-3-642-20573-6_67

[6] Dr.S.S.Dhenakaran and A.Parvathavarthini, "An Overview of Routing Protocols in Mobile Ad-Hoc Network", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, 2013

[7] C. Zhang, Y. Song, Y. Fang, and Y. Zhang, "On the price of security in large-scale wireless ad hoc networks", IEEE/ACM Trans. Netw., vol. 19, no. 2, pp. 319–332, Apr. 2011. https://doi.org/10.1109/TNET.2011.2106162

[8] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs", in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222. https://doi.org/10.1145/1967486.1967522

[9] W. Liang and W. Wang, "A Quantitative Study of Authentication Networks", Proc. IEEE INFOCOM, vol. 2, pp. 1478-1489, 2005.

[10] C.E. Perkins and E.M. Royer, "Ad-Hoc On-Demand Distance Vector Routing", Proc. 2nd IEEE Workshop Mobile Computing Systems and Applications (WMCSA'99), IEEE Press, 1999, pp. 90–100. https://doi.org/10.1109/MCSA.1999.749281

[11] W. Wang, W. Liang, and A.K. Agarwal, "Integration of Authentication and Mobility Management in Third Generation and WLAN Data Networks", Wireless Comm. and Mobile Computing (WCMC), special issue on WLAN/3G integration for next-generation heterogeneous mobile data networks, vol. 5, no. 6, pp. 665-678, Sept. 2005.
[12] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review", Int'l J. Computer Applications, vol. 12, no. 2, pp. 37-43, Dec. 2010.
[13] V. Kumar and M.L. Das, "Securing Wireless Sensor Networks with Public Key Techniques", Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.
[14] A. Noack and S. Spitz, "Dynamic Threshold Cryptosystem without Group Manager", Network Protocols and Algorithms, vol. 1, no. 1, Oct. 2009.
[15] J. Yan, J. Ma, F. Li, and S.J. Moon, "Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks", Ad Hoc and Sensor Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.
[16] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs", IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007. https://doi.org/10.1109/TMC.2007.1036
[17] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Proc. 8th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom 2002), ACM Press, 2002, pp. 12–23. https://doi.org/10.1145/570645.570648
[18] L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems", Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.
[19] Guoxing Zhan, Weisong Shi, and Julia Deng. Design and implementation of tarf: A trust-aware routing framework for wsns. IEEE Transactions on Dependable and Secure Computing, 9(2):184–197, 2012. https://doi.org/10.1109/TDSC.2011.58
[20] Latvakoski J., D. Pakkala, and P. Paakkonen, "A Communication Architecture for Spontaneous Systems", IEEE Wireless Comm., vol. 11, no. 3, pp. 36-42, June 2004. https://doi.org/10.1109/MWC.2004.1308947
[21] Feeney L.M., B. Ahlgren, A. Westerlund, and A. Dunkels, "Spontnet: Experiences in Configuring and Securing Small Ad Hoc Networks", Proc. Fifth Int'l Workshop Network Appliances, Oct. 2002.
[22] Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast", in Proc. Network Distributed System Security Symposium (NDSS'01), pp. 35-46, Feb. 2001.
[23] J. Sun, C. Zhang, Y. Zhang, and Y. (Michael) Fang, "An Identity- Based Security System for User Privacy in Vehicular Ad Hoc Networks", IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010. https://doi.org/10.1109/TPDS.2010.14
[24] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks", IEEE Wireless Communications Magazine, special issue on Security in Wireless Mobile Ad Hoc and Sensor Networks, Vol.14, No.5, pp. 56-63, Oct. 2007.

7 Authors

L. Raghavendar Raju is with Matrusri Engineering College, Hyderabad, India, email: lraghavenderraju@gmail.com

Dr. C. R. K. Reddy is with Chaitanya Bharathi Institute of Technology, Hyderabad, India, email: crkreddy@cbit.ac.in

Article submitted 25 November 2016. Published as resubmitted by the authors 23 January 2017.