Ensuring Data Confidentiality and Privacy in Mobile Ad Hoc Networks

Hamza Aldabbas[1], Helge Janicke[1], Radwan AbuJassar[2], and Tariq Alwada'n[1]

[1] Software Technology Research Laboratory (STRL), De Montfort University, Leicester, United Kingdom
{hamza,heljanic,tariq}@dmu.ac.uk
[2] School of Computer Science and Electronic Engineering, University of Essex, Essex
{rabuja}@essex.ac.uk

Abstract. Mobile *ad hoc* networks (MANETs) are autonomous systems which are comprised of a number of mobile nodes that communicate between themselves by wireless communication in a peer-to-peer basis. They are self-organized, self-configured and self-controlled infrastructure-less networks. Nodes can communicate with each other without any pre-planned or a base station. Disseminating information securely between these nodes in such networks however is a challenging task, particularly when the information is confidential. Revealing such information to anyone else other than the intended nodes could be highly damaging, especially in military applications where keeping the message secret from adversaries is essential. In this paper we present our novel framework for privacy control in mobile *ad hoc* networks in which privacy policies are attached to messages as they are send between peers. We evaluate our framework using the Network Simulator (NS-2) to provide and check whether the privacy and confidentiality of the originator are met. For this we implemented the privacy enforcement as an NS2 agent that manages and enforces the policies attached to packets at every node in the MANET.

Keywords: MANETs, Policy Enforcement Point(PEP), Policy decision Point(PDP) and Discretionary Access Control (DAC).

1 Introduction

Recently, mobile *ad hoc* networks received extensive attention in both industrial and military applications, because of the striking property of creating a network while moving from one place to another and it does not require any pre designed infrastructure. The key challenges in designing (MANETs) come from the decentralised nature, self-organisation, and self-management, since the opportunity of the node movement is very high. On top of that, all communications are carried out through wireless medium in short-range communication. These unique characteristics present some security issues for (MANETs), so there have been concerted efforts by the research community [13,3,14] in message encryption, digital signature, key management etc. Many challenges especially related to the privacy of originator issues however remain to be solved.

N. Meghanathan et al. (Eds.): CCSIT 2012, Part I, LNICST 84, pp. 490–499, 2012.

These existing approaches in security which have been applied to MANETs such as access control, digital signature, and encryption focused only in securing the channel, however how these nodes act after these mechanisms is left.

In this paper we provide a review of the security issues in MANET and survey existing solutions for this problem and to highlight a particular area which has not been addressed up to now which is controlling the information flow in mobile ad hoc networks, and to provide an architecture that allows the policy-based control the dissemination of data that is communicated between nodes, in order to ensure that data remains confidential not only during transmission but also after it has been communicated to another peer, to keep message contents private to an originator defined subset of nodes in the MANET.

We will overview the characteristics in MANETs in Section 2, and focus on security issues in Section 3. In Section 4 we present the state of the art work on securing (MANETs) to which we relate our proposed policy-based architecture and the algorithim chart in Section 5, then the discussion will be presented in section 6. The paper concludes in section 7 where we summarise our findings and outline our future work in this area.

2 Characteristics of MANET

A mobile *ad hoc* network (MANET) is an independent system of mobile nodes linked by wireless connections. These nodes are thus free to move arbitrarily; therefore, the topology of wireless networks can be changed swiftly and in an unpredictable manner. MANETs have therefore many characteristics that make them are distinguished from other wireless and wired networks [1,9,12,4] which in detail are:

1. **Constrained Resources:** In general, most MANET devices are small handheld devices like personal digital assistants (PDAs), laptops and cell phones. These devices indeed have limitations because of their restricted nature battery-operated, small processing and storage facilities.
2. **Infrastructure less(Autonomous):** MANETs are created based on the teamwork between independent nodes, peer-to-peer nodes that need to communicate with each other for some aim. Without any pre-planned or base station.
3. **Dynamic Topology:** MANET nodes can move arbitrarily; thus the nodes can be dynamically inside and outside the network, continually changing its links and topology, leads to change in the routing information all the time due to the movement of the nodes. Consequently, the communicated links between nodes could be bi-directional or unidirectional.
4. **Limited Physical Security:** MANETs are in general more vulnerable to physical layer's attacks than wired network; the possibility of spoofing, eavesdropping, jamming and denial of service (DoS) attacks should be carefully considered. However the self-administration nature of MANET makes them more robust against single failure points.
5. **Short Range Connectivity:** MANETs rely on radio frequency (RF) technology to connect, which is in general considered to be short range communication. For that reason, the nodes that want to communicate directly need to be in the close

frequency range of each other. In order to tackle this limitation, multi-hop routing mechanisms have therefore to be used to link remote nodes through intermediary ones that operate as routers.

3 Network Security

The distinctive characteristics of MANETs bring a new set of essential challenges to security design, these challenges noticeably make the looking for security solutions that perform both data protection and applicable network performance are required [11]. Normally while we addressing the network security, we have to consider the security requirements to take account of the functionality required to provide a secure networking system.

3.1 Security Requirements

The security requirements specified below specified by International Telecommunications Union (ITU-T) represented in their recommendation X.805 and X.800 [8,7,11]:

1. **Authentication:** Authentication is very important to verify the identity of each node in MANET and its eligibility to access the network. This means that, nodes in MANETs are required to verify the identities of the communicated entities in the network, to make sure that these nodes are communicating with the correct entity.
2. **Authorisation and Access Control:** Each node in MANET is required to have the access to shared resources, services and personal information on the network. In addition, nodes should be capable of restricting each other from accessing their private information. There are many techniques that can be used for access control such as Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Based Access Control (RBAC).
3. **Privacy and confidentiality:** Each node has to secure both the information that is exchanged between each other; and secure the location information and the data stored on these nodes. Privacy means preventing the identity and the location of the nodes from being disclosed to any other entities, while confidentiality means keeping the secrecy of the exchanged data from being revealed to those who have not permission to access it.
4. **Availability and survivability:** The network services and applications in MANET should be accessible, when needed, even in the presence of faults or malicious attack such as denial-of-service attack (DoS). While survivability means the capability of the network to restore its normal services under such these conditions. These two requirements should be supported in MANET.
5. **Data integrity:** The data transmitted between nodes in MANET should be received to the intended entities without been tampered with or changed by unauthorised modification. This requirement is essential especially in military, banking and aircraft control systems, where data modification would make potential damage.
6. **Non-repudiation:** This ensures that nodes in MANET when sending or receiving data-packets should not be able to deny their responsibilities of those actions. This

requirement is essential especially when disputes are investigated to determine the misbehaved entity. Therefore digital signature technique is used to achieve this requirement to prove that the message was received from or sent by the alleged node.

4 State of the Art

Existing approaches in security which have been applied to MANETs. For example, traditional cryptographic solutions are using public key certificates to maintain trust, in which a Trusted Third Party (TTP) or Certificate Authority (CA) certifies the identity associated with a public key of each communicated entities, therefore they can provide end-to-end secure communication channels. These approaches mainly focused on message confidentiality, integrity and non-repudiation, they do not consider however the trust management of the communicated entities, and how these certified entities act is left to the application layer [2]. Lidong Zhou et al [14] studied the security threats, variabilities and challenges which faces the ad hoc network, in their work they protected the packets sent between nodes by choosing the secure routing path to the destination node based on the redundancies routes between nodes to maintain the availability requirement, because of all key based cryptographic approaches such as digital signature needs a proper and secure key management scheme to bind between the public and private keys to the nodes in the network; Lidong Zhou used replication and new cryptographic technique (threshold cryptography) [6,5] to build a secure key management process to achieve the trust between a set of servers in ad hoc networks by distributing trust among aggregation of nodes to certify nodes are trustworthy.

Securing the routing in mobile ad hoc network has also given much interest by the researchers; therefore many approaches have been proposed to cope with external attack. Sirios and Kent [10] proposed an approach to protect the packet sent to multi receivers by using keyed one-way hash function supported by windowed sequence number to ensure data integrity . The trust issue systems like in mobile ad hoc network is a challenging task to achieve. Whilst Public Key Infrastructure (PKI) and cryptography are achieving kind of a quasi-trust before the communication is start. However how the nodes act after that will be controversial issue as you cannot predict who is going to be un trusted node only on the behaviour without using a tracing technique to prove some nodes are misbehaving in the network and thus they are un trusted anymore.

In our work we show how disclosing private information by a malicious node (inside the network) to unauthorised nodes will cause a fatal problem and data will be leaked. Therefore traditional encryption tools are widely used in security systems and it solved part of the problem by encrypting data exchanged between entities by encrypting in the public key of the destination node and then decrypting the packet by the destination's private key but how the distination behave after is left. However, using the mechanisim which using the access control to ensure confidentiality is still not been used, so our work intend to use access control mechanism especially Discretionary Access Control (DAC) to ensure data confidentiality and privacy of the originator node in MANETs.

5 Our Proposed Framework

5.1 Scenario

Protecting a message sent in wireless network such as in mobile *ad hoc* networks (MANETs) is a very difficult task. For example, in military alliance where some armies want to share tactical mission information only between themselves and not with other coalition members.

Considering three nodes A,B,C in Figure 1, where node A and B are allocated to British and US armies, and C is allocated to Afghan army. Node A wants to send a tactical message for the mission that says "'we are going to start the mission after 8 pm"' to node B, however node A does not want node B send the message to nodeC because node C is not trusted by A. How can node A trust node B not to send the message to node C?

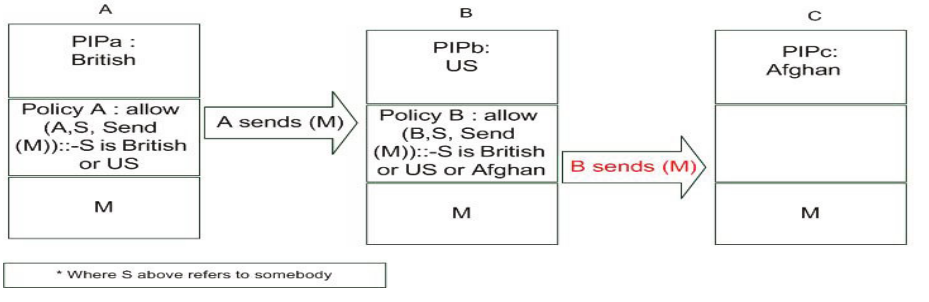

Fig. 1. node B disclose the message to C

Node A sends the message (M) to node B, node B now knows the message (M). However depend on its policy node B can send the message (M) and disclose it to node C. Which it is the problem of the node A privacy.

The goal of our proposed approach is to solve this problem by allowing the originator to specify a high level policy which will automatically apply and enforce itself to all the communicated entities on the network. This is done by attaching the policy of the originator (A) with the message (M) to control the access to it, which is capable to define who are allowed to access that message. In this way the policy of node A attached with the message (M), tells node B to which node can the message (M) be send to (only British or US armies can receive the message) as in Figure 2 :

Node A sends the message (M) + policy of node A which tells node B to allow sending the message (M) to any node if its British or US nodes. Here after node A sent the message (M) to node B attached by the node A policy. node B receives the packet and now knows the message (M) in addition of that it knows the policy of A':

Allow (Node B, Send(M) to S: if S is British or US, where S refers to somebody.

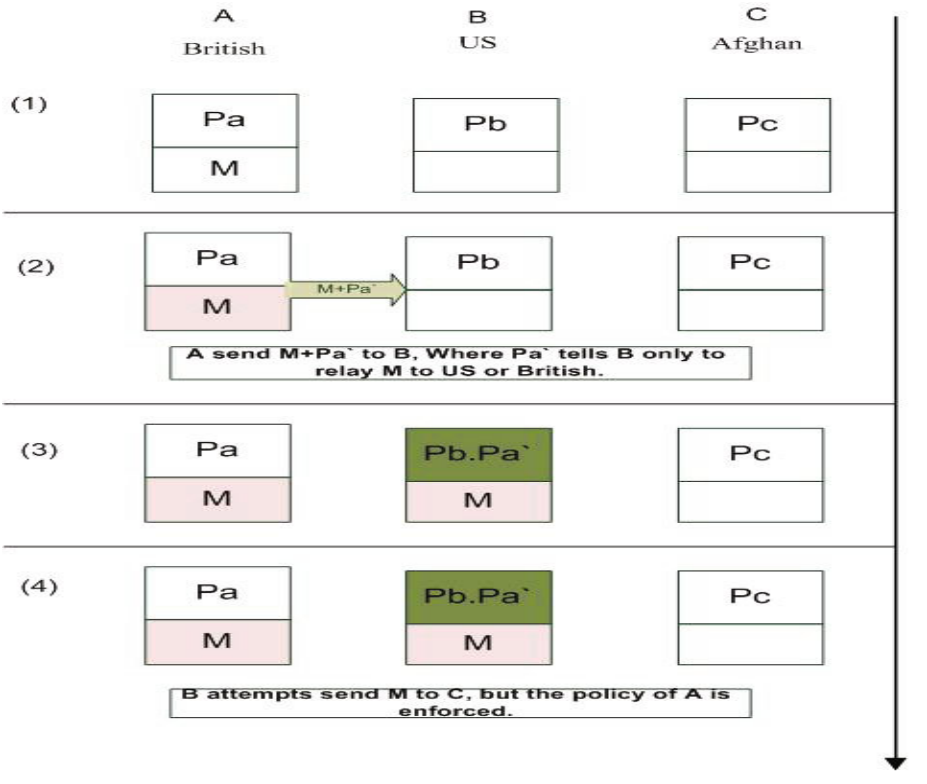

Fig. 2. Prevention Node B Of Disclosing M to node C

5.2 Our Framework

Figure 3 presents the proposed framework, where policies are used to enforce access control to such information sent by the originator to other entities in the system, our framework will be introduced in every entity in the communicated systems.

Our framework is composed of four components as they shown in the Figure 3:

1. policy enforcement point (PEP/OUT): executes and enforces policy decisions in the sender node, this component installed at the transmitter interface that does merge system's policy with the message sent to others systems. In our simulation we configured the send function to achieve the functionalities of this component.
2. policy enforcement point (PEP/IN): executes and enforces policy decisions in the receiver node, this component installed at the receiving interface that does inverse process at the receptive system, splitting and dividing the message from the policy attached. In our simulation we configured the receive function to achieve the functionalities of this component.
3. Policy decision point (PDP): plays a crucial role in both the sender and the receiver side in our framework, and helping other components to do their jobs. In our simulation we configured this function at the source to achieve the functionalities of this component.

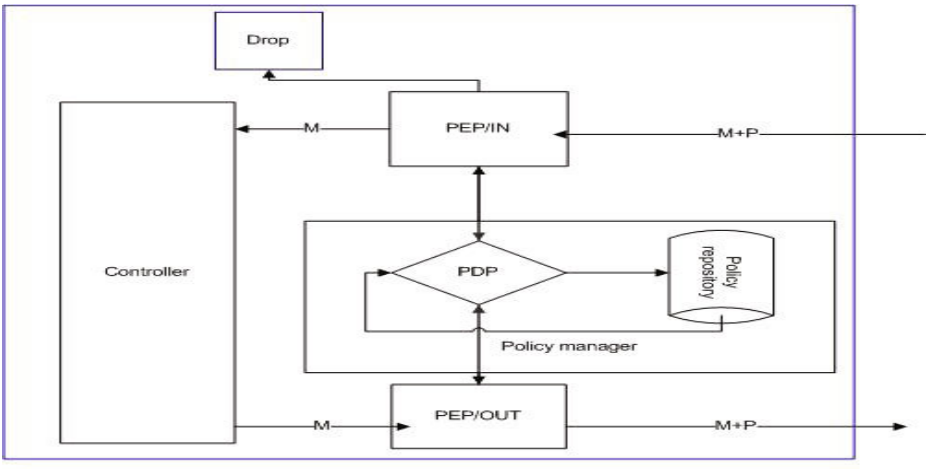

Fig. 3. The proposed framework

4. controller that process and store the information received from the other components.

In the Figure 4 we show an example of six nodes, assuming that each node in the system has a grouipid number, that means we are classifying the nodes in our work into different groups, which in such case are three groups: groupid1, groupid2, groupid3. The first group has n0,n2,n4 and n5. where as n1 and n3 are in groupid3 and groupid3 respectively. In our work we make n0 broadcast a message to all nodes in the groupid which specified in the policy file at file0.txt in node n0, and we call this grouipid in this situation is permitted group as shown in the algorithm chart in Figure 5. If file0.txt as in the example has 1 that means only nodes in the groupid1 can recieve the pkt.

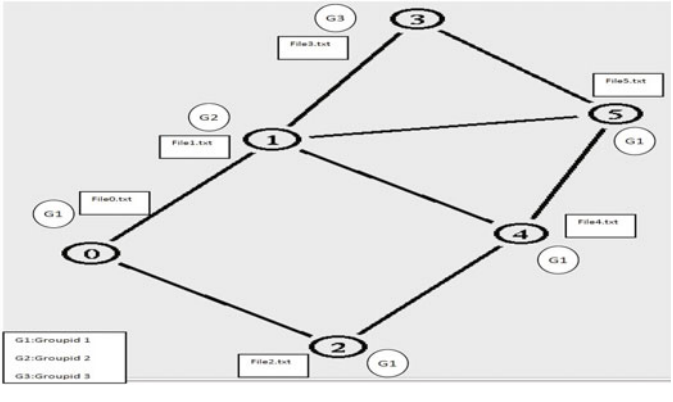

Fig. 4. Example illustrating the Algorithim chart

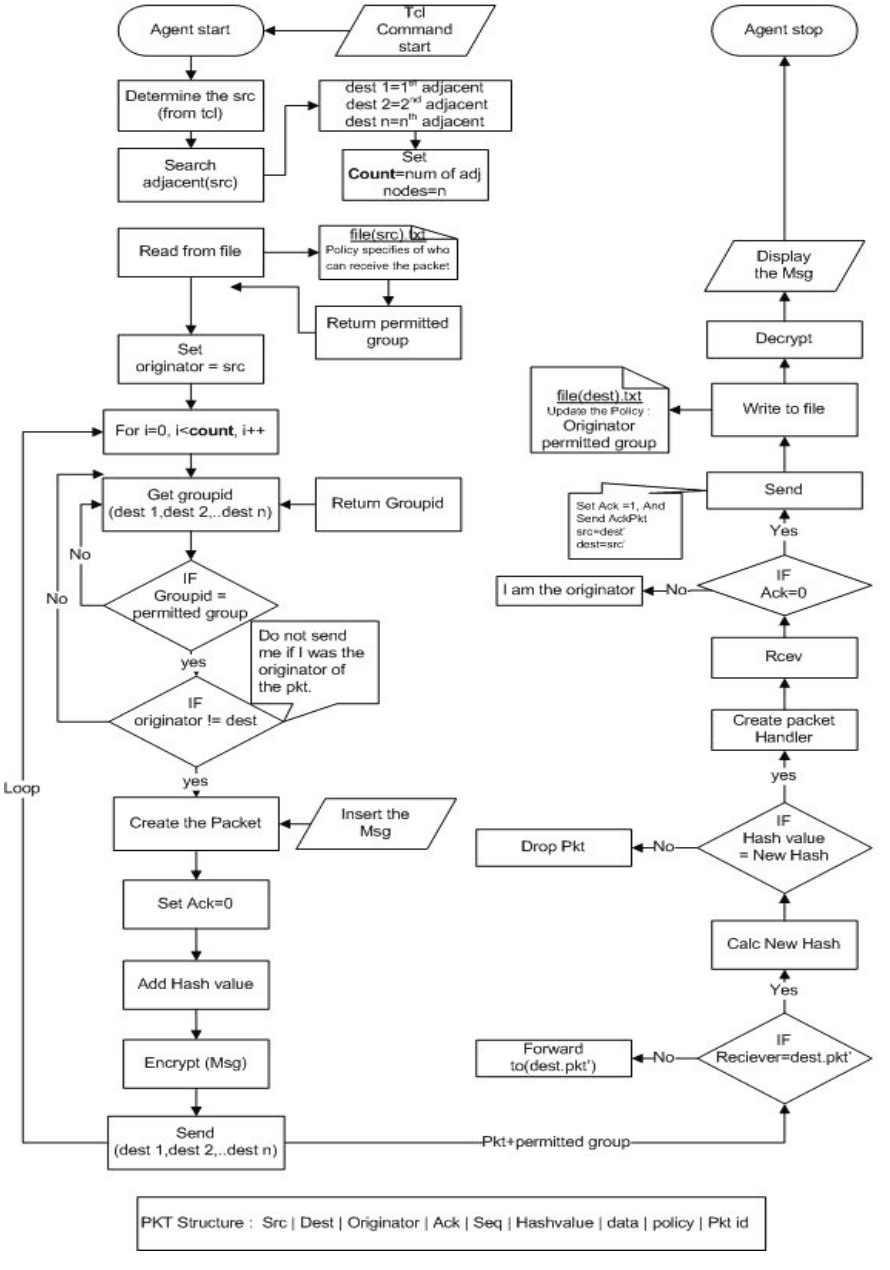

Fig. 5. Our Chart Algorithim and packet structure

Then n0 will start searching for the adjacent nodes in the range. In this example n0 will find n1 and n2. dest1=n1 dest2=n2. Now n0 will check if the dest1 in the permitted group or not and do the same to dest2 also. In the algorithm chart this depicted as Getgroupid (dest) process and check If groupid=permitted group or not. In this example it will be yes for n2 as n2 in the groupid1. n0 will send to n2 not only the pkt it also sends his policy which existed in file0.txt, where as n2 will create a packet handler to recieve the pkt, once it recieved the policy of n2 will be updated according to policy of n0 and deletes it's old policy becuasue it is the originator policy.

Now, when n2 at another time wants to broadcast the message again will start and do the same process like in n0, however this time n2 will send to n4 but not to n0 becasue n0 is the originator of the pkt as shown in the algorithm chart in Figure 5, and the system will continue in the same steps for other nodes.

6 Result and Discussion

In this work we used the Network Simulator (NS2) which is a real network environment simulator, which showed only intended nodes can recieve the packet which has been sent by the source. We simulated our approach into multi variable number of nodes where the originator node disseminate the packet(Data+Policy) to the other nodes. Our result from the tracing file and the nam showed that only nodes in the permitted groupid can recieve the packet, because of the restriction which has issued from the originator node 'not to send the packet to nodes in different groupid '.

We simulated our agent with the vary number of UDP agents together to check what if all agents are started in the simulation and how that will be affect the time taken for a packet to be transmitted across a network from source to destination. In Figure 6 we measured the delay time versus number of cbr traffics which depicted on the y-axis and x-axis respectively, the result of this figure showed that as the the number of cbr traffic

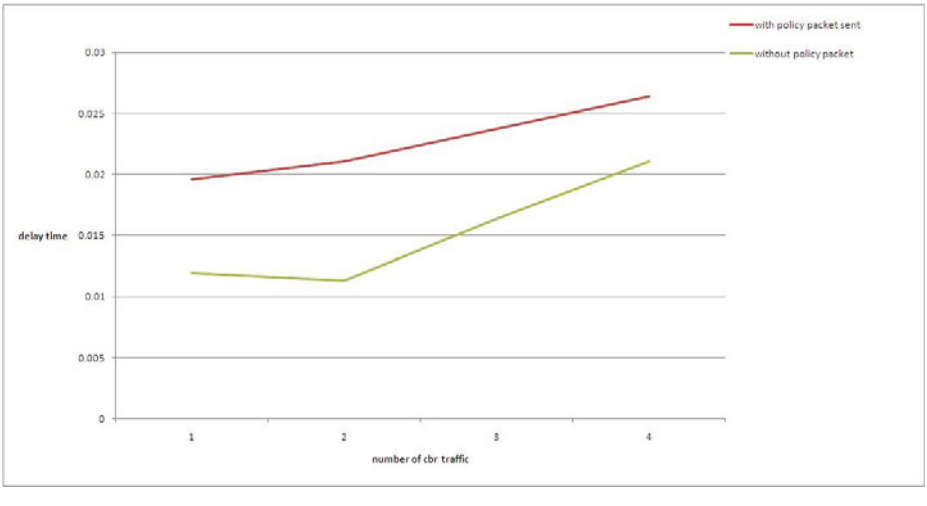

Fig. 6. Delay time

increase, the delay time of both agents will increase, we started with 1 cbr traffic, 2 3 and 4 with and without our agent be started at different sources and destinations to measure the average of the delay time between them.

7 Conclusion

In this paper we concluded that our framework acheived the source policy to send the packet for intended nodes only in the network, on top of that we highlighted the special considerations for security in MANETs and provided an extensive overview of related work and the state of the art in this area. To our knowledge, none of the related work addressed the issue of controlling the information flow in mobile *ad hoc* Networks. We presented a scenario drawn from the military domain, where the impact of this form of confidentiality breach is evident and a real risk. We provided an architecture that addresses this problem by automatically attaching policies to the messages that identify how the information can be used by the receiver, thus limiting the relay of messages based on the originator's confidentiality requirements.

References

1. Al-Jaroodi, J.: Security issues at the network layer in wireless mobile ad hoc networks at the network layer. Tech. rep., Faculty of Computer Science and Engineering, University of Nebraska-lincoln, Nebraska, USA (2002)
2. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. In: Proceedings of 1996 IEEE Symposium on Security and Privacy, pp. 164–173. IEEE (1996)
3. Burbank, J., Chimento, P., Haberman, B., Kasch, W.: Key challenges of military tactical networking and the elusive promise of manet technology. IEEE Communications Magazine 44(11), 39–45 (2006)
4. Chadha, R., Kant, L.: Policy-driven mobile ad hoc network management. Wiley-IEEE Press (2007)
5. Desmedt, Y., Frankel, Y.: Threshold Cryptosystems. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 307–315. Springer, Heidelberg (1990)
6. Desmedt, Y.: Threshold cryptography. European Transactions on Telecommunications 5(4), 449–458 (1994)
7. Li, W., Joshi, A.: Security Issues in Mobile Ad Hoc Networks-A Survey (2008)
8. Menezes, A., Van Oorschot, P., Vanstone, S.: Handbook of applied cryptography. CRC (1997)
9. Murthy, C.S.R., Manoj, B.: Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall PTR, Upper Saddle River (2004)
10. Sirois, K., Kent, S.: Securing the nimrod routing architecture. In: SNDSS, p. 74. IEEE Computer Society (1997)
11. Stallings, W.: Cryptography and Network Security: Principles and Practice, 4th edn. Pearson Education (2005)
12. Toh, C.: Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks. IEEE Communications Magazine 39(6), 138–147 (2001)
13. Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L.: Security in mobile ad hoc networks: challenges and solutions. IEEE Wireless Communications 11(1), 38–47 (2004)
14. Zhou, L., Haas, Z.: Securing ad hoc networks. IEEE Network 13(6), 24–30 (1999)