A VIEW ON SECURE ROUTING IN ADHOC NETWORKS

V. Venkata Ramana[1]
Asst. Prof., CSE Dept.,
SSITS, Raychoti,
Kadapa (dist), A.P. INDIA.

K.K.Basheer[2]
Asst.Prof. CSE Dept.,
VITS, Proddatur.
Kadapa (dist), A.P. INDIA.

P.Srinivasa Rao[3]
Asst. Prof, CSE Dept.,
GMRIT, Rajam, Srikakulam(dist)
A.P.,INDIA.

ABSTRACT

In our proposed research work different security attacks from the perspective of layer approach are identified. The impacts of security attacks on each layer are studied. Then we focus on security attacks on network layer in particular routing. Different solutions for different security attacks will be proposed. For this widely proposed Adhoc network routing protocols DSR and AODV are used.

KEYWORDS

Adhocnetworks,Attack,Bandwidth,DSR,DSDV,Certificate.

1. INTRODUCTION

An Adhoc network is a collection of mobile nodes forming a temporary network with out any additional infrastructure and no centralized control. Some of the applications of Adhoc networks are disaster management during earthquakes, military applications, students in a class room sharing information and floods etc. Adhoc network can be created on the fly each node in the Adhoc network acts both as a router and host. Adhoc network otherwise called as reconfigurable network.

1.1. Characteristics of Wireless networks

Relatively wired networks have the characteristics and their use field proven Technology. With wide use of fiber optics, wired networks have abundant bandwidth. Probability of error is negligible. But the link characteristics in wireless networks are different from that of wired networks. Some of the characteristics of wireless Networks are as follows.

Bandwidth: bandwidth is one of the scarcest resources in wireless networks. Typical available band width in wireless networks (2-10 Mbps) is far less than that of wired networks (1Gbs).

Range Issues: In wired networks data can be transmitted over large distance without attenuation. This is not the case with wireless networks. Radio signals suffers from various transmission impairments and typical range is in meters.

Power: The wireless nodes are battery operated and therefore nodes reduce the power at which they transmit to conserve energy. Also the power at which nodes transmit is to be controlled to reduce interference.

Collisions: Since all nodes can not listen to each other, simultaneous transmission by the nodes may result in collision.

Link Errors: the probability of errors in wireless environment is high. As they are more susceptibility to environmental conditions.

Unpredictable Link Properties: Wireless links are very unpredictable.

Bandwidth available varies with environmental conditions. Signal propagation faces difficulties such as signal fading interference, and multi-path cancellation.

1.2. Characteristics of Adhoc networks

Apart from the characteristics mentioned above, Adhoc networks have some characteristics which make them different from wired and wireless networks. They are as follows.

Mobility Induced Link Breakages: As the nodes in an Adhoc network are usually mobile, the nodes may go out of range of neighboring nodes resulting in break in the links between the nodes. These may leads to break in the route between source and destination nodes.

Sleep Period of Operation: To conserve energy, nodes in an Adhoc network may enter inactive state where by they do not transmit at some instants of time.

Highly Unfavorable environmental conditions: Adhoc networks are generally used in environments which are highly unfavorable for transmission and reception.

Looping Problem: Due to mobility temporary loops may result.

Misbehavior: Some nodes may misbehave transmitting their own data and refusing to transmit data from other nodes. Since Adhoc network uses multi hop routing this has to be controlled.

Addressing Problem: In an Adhoc network is not possible to have fixed nodes Acting as DHCP server, but nevertheless. All the nodes should follow a uniform addressing mechanism.

2. Classification of Routing Protocols

Routing in Adhoc network is a non trivial task. Routing protocols are in Adhoc networks can be classified in to two types.

1. Proactive Routing protocols
2. Reactive Routing protocols.

In proactive routing protocols nodes pre-compute the roots by exchange information periodically. Examples are Destination Sequenced Distance Vector (DSDV) routing.

In reactive routing protocols routes are pre-computed. Examples are Dynamic Source Routing (DSR), Adhoc on demand distance vector routing etc. **3.GOals of a Security System**

1) Availability: Ensures survivability despite Denial Of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

2) Confidentiality: Ensures certain information is never disclosed to unauthorized entities.

3) Integrity: Message being transmitted is never corrupted.

4) Authentication: Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

5) Non-repudiation Ensures that the origin of a message cannot deny having sent the message.

4. Security Issues

Attacks:

Use of wireless links renders an Adhoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Eavesdropping might give an attacker access to secret information thus violating confidentiality. Active attacks could range from deleting messages, injecting erroneous messages, impersonate a node etc thus violating availability, integrity, authentication and non-repudiation. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, we need to consider malicious attacks not only from outside but also from within the network from compromised nodes. For high survivability Adhoc networks should have a distributed architecture with no central entities, centrality increases vulnerability. Ad-hoc network is dynamic due to frequent changes in topology. Even the trust relationships among individual nodes also changes, especially when some nodes are found to be compromised. Security mechanism need to be on the fly(dynamic) and not static and should be scalable.

Key Management

Cryptographic schemes such as digital signatures are often employed to protect both routing information as well as data. Public key systems are generally espoused because of its upper hand in key distribution.

Distance Vector Routing Algorithm

Distance Vector Routing algorithms are also known as Bellman-Ford routing algorithms and Ford-Fulkerson routing algorithms. Distance Vector Routing Algorithms operate by having each router maintain a table or a vector giving the best known distance to each destination and which line to use to get there. This approach assigns a number, the cost, to each of the links between each node in the network. Nodes will send information from source to destination via the path that result in the lowest total costs.

Secure Routing

The main assumption of the previously presented Adhoc routing protocols is that all participating nodes do so in good faith and without maliciously disrupting the operation of the protocol . However, the existence of malicious entities cannot be disregarded in any system, especially in open ones like Adhoc networks. The RPSEC IETF working group has performed a threat analysis that is applicable to routing protocols employed in a wide range of application scenarios . According to this work, the routing function can be disrupted by *internal* or *external* attackers. An internal attacker can be any legitimate participant of the routing protocol. An external attacker is defined as any other entity.

The strongest assumption for an external attacker is that it is able to eavesdrop the communication between two legitimate network participants, inject fabricated messages and delete, alter or replay captured packets. Weaker assumptions of external attackers include the ability to inject messages but not read them, or read and replay messages but not inject new ones, or just the ability to read messages. Cryptographic solutions can be employed to prevent the impact of external attackers by mutual authentication of the participating nodes through digital signature schemes. However, the underlying protocols should also be considered since an attacker could manipulate a lower level protocol to interrupt a security mechanism in a higher level.

Internal attackers have the capabilities of the strongest outside attacker, as they are legitimate participants of the routing process. Having complete access to the communication link they are able to advertise false routing information at will and force arbitrary routing decisions on their peers . One of the most difficult to detect problems in routing is that of *Byzantine failures*. These failures are the result of nodes that behave in a way that does not comply with the protocol. The reasons for the erroneous behavior could be software or hardware faults, mistakes in the configuration, or malicious compromises. Attempts to solve the problem of Byzantine failures have been proposed for both infrastructure and infrastructure less networks.

5. Specific attacks in routing protocols

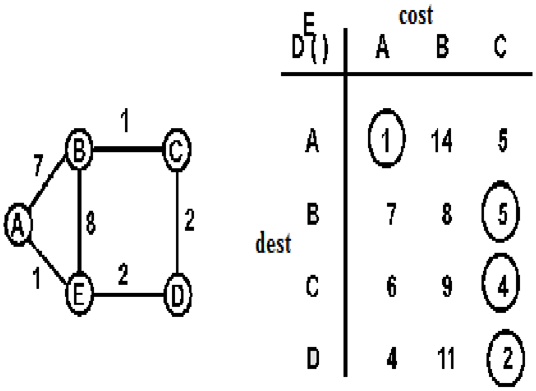
- Location ***disclosure***: Location disclosure is an attack that targets the privacy requirements of an Adhoc network. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches an attacker is able to discover the location of a node, or even the structure of the entire network.
- ***Black hole*** : In a black hole attack a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.
- ***Replay****:* An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.
- ***Wormhole****:* The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network. One attacker, say node A, captures routing traffic at one point of the network and tunnels them to another point in the network, say to node B, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers.
- ***Blackmail*****:** This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated .

Denial of service: Denial of service attacks aim at the complete disruption of the routing function and therefore the whole operation of the Adhoc network. Specific instances of denial of service attacks include the *routing table overflow* and the *sleep deprivation torture* . In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

- ***Routing table poisoning*****:** Routing protocols maintain tables which hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the Adhoc network. Routing table poisoning attacks can result in selection of non-optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network.

6. Existing Solutions to Secure Routing

There exist several proposals that attempt to architect a secure routing protocol for Adhoc networks, in order to offer protection against the attacks mentioned in the previous section. These proposed solutions are either completely new stand-alone protocols, or in some cases incorporations of security mechanisms into existing ones (like DSR and AODV). The design of these solutions focuses on providing countermeasures against specific attacks, or sets of attacks. Furthermore, a common design principle in all the examined proposals is the performance-security trade-off balance.



$D^E()$	A	B	C
A	1	14	5
B	7	8	5
C	6	9	4
D	4	11	2

Fig.1: DVR Example

Since routing is an essential function of Adhoc networks, the integrated security procedures should not hinder its operation. Another important part of the analysis is the examination of the assumptions and the requirements that each solution depends on. Although a protocol might be able to satisfy certain security constraints, its operational requirements might thwart its successful employment.

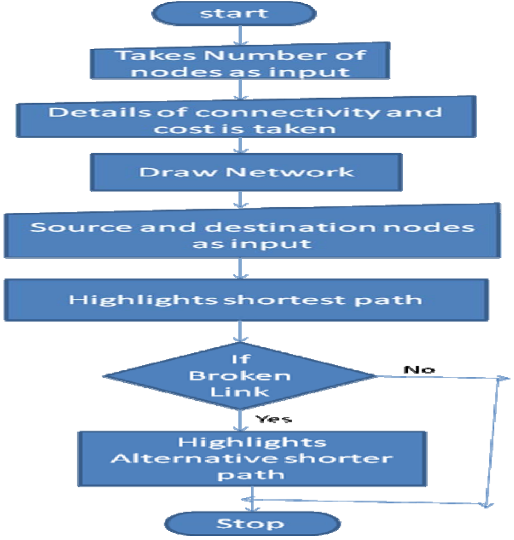

start
Takes Number of nodes as input
Details of connectivity and cost is taken
Draw Network
Source and destination nodes as input
Highlights shortest path
If Broken Link
No
Yes
Highlights Alternative shorter path
Stop

Fig.2 : DVR Flowchart

In order to analyze the proposed solutions in a structured way they are classified into five categories; solutions based on asymmetric cryptography, solutions based on symmetric cryptography, hybrid solutions and a category of mechanisms that provide security. However, this classification is only indicative since a lot of solutions can be classified into more than one category.

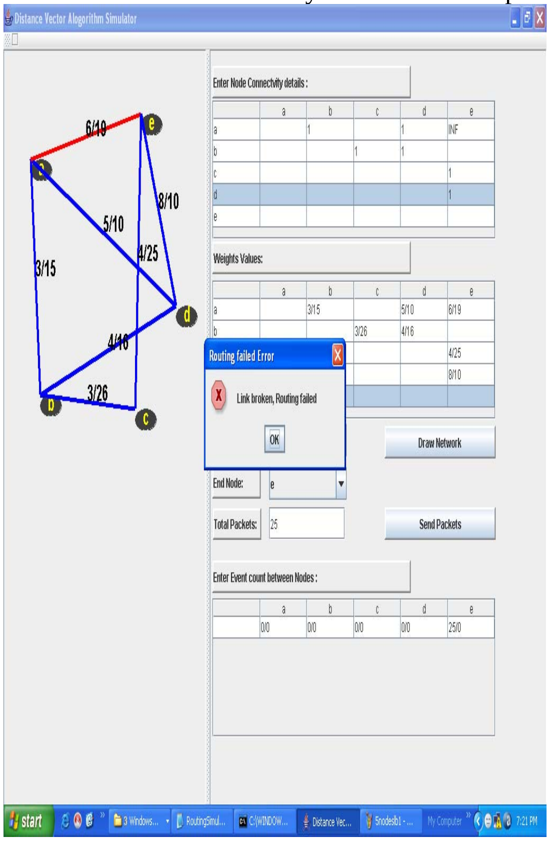
1.1.1 *Symmetric Cryptography Solutions*

This category presents solutions that rely solely on symmetric cryptography to secure the function of routing in wireless Adhoc networks. The most commonly utilized mechanisms are *hash functions* and *hash chains*. A one-way hash function is a function that takes an input of arbitrary length and returns an output of fixed length.

Hash functions have the property of being computationally expensive to reverse i.e. if *h* = *f(m)*, it is hard to compute *m* such as *f(m)* = *h*. There are several well-known hash functions that possess these properties such as SHA-1 and MD5 . A hash chain can be generated by applying repeatedly a given hash function to a random number known as the *root* of the chain. Simply stated, in order to generate a hash chain of length *n* hash function is applied *n* times to a random value *p*, and the final hash *q* that is obtained is called the *anchor* of the chain. In order to use a hash chain for authentication purposes an initial authenticated element of the chain is assumed, usually the anchor. Given this it is possible to verify the authenticity of the elements that come later in the sequence. Since hash functions are especially lightweight when compared to other symmetric and asymmetric cryptographic operations, they have been extensively used in the context of securing Adhoc routing and specifically in hop count authentication providing countermeasures against specific attacks, or sets of attacks

1.1.2 *Asymmetric Cryptography Solutions*

Protocols that use asymmetric cryptography to secure routing in mobile Adhoc networks require the existence of a universally trusted third party (TTP). TTP issues certificates that bind a node’s public key with a node’s persistent identifier. Furthermore, the TTP can be either online or offline. In approaches that use an online TTP, revocation of the issued certificates is accomplished by broadcasting certificate revocation lists (CRLs) in the network. In offline systems revocation becomes a particularly complicated problem and usually involves the exchange of recommendations between the participating nodes.



Enter Node Connectvity details :

	a	b	c	d	e
a		1		1	INF
b			1	1	
c					1
d					1
e					

Weights Values:

	a	b	c	d	e
a		3/15		5/10	6/19
b			3/26	4/16	
					4/25
					8/10

Routing failed Error

Link broken, Routing failed

OK

End Node: e

Total Packets: 25

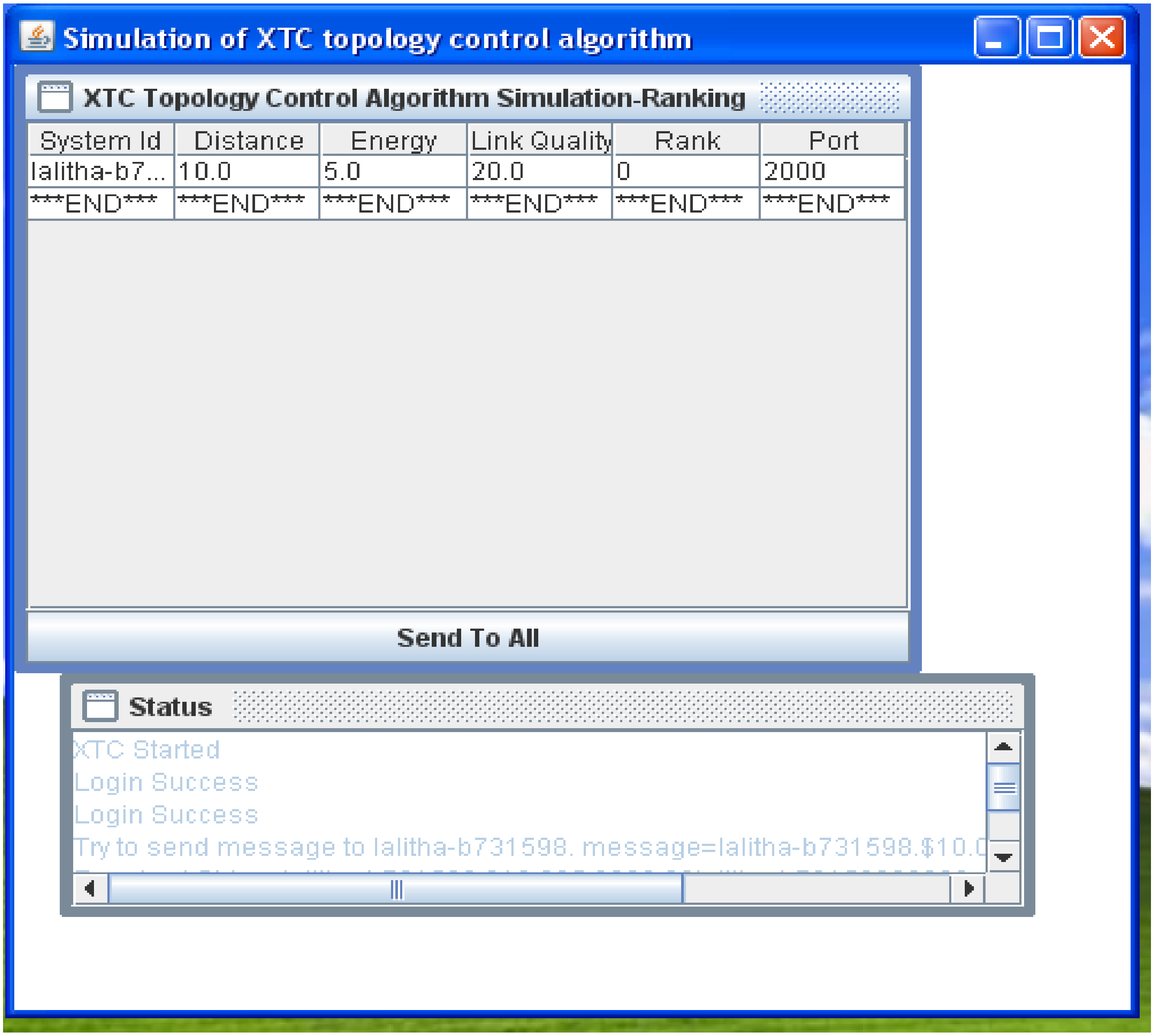
Enter Event count between Nodes :

	a	b	c	d	e
	0/0	0/0	0/0	0/0	25/0

Fig. 3: Broken link

1.1.3 *Hybrid Solutions*

In this category secure routing protocols employ both symmetric and asymmetric cryptographic operations. The most common approach is to digitally sign the immutable fields of routing messages in order to provide integrity and authentication, and to use hash chains to protect the hop count metric.


Simulation of XTC topology control algorithm
XTC Topology Control Algorithm Simulation-Ranking
Send To All
Status

System Id	Distance	Energy	Link Quality	Rank	Port
lalitha-b7...	10.0	5.0	20.0	0	2000
END	***END***	***END***	***END***	***END***	***END***

```
XTC Started
Login Success
Login Success
Try to send message to lalitha-b731598. message=lalitha-b731598.$10.0
```

Fig.4: rank calculation using XTC.

Conclusion

Cannot assure for confirmed data transmission are rectified using this system. It provides confirmed transmission of data, reduction of network density, and lesser consumption of energy, reduced bandwidth, portable network irrespective of geographical area and elimination of congestion. Each different scenario has its own set of security requirements and demands from the underlying routing protocol. Hence, an additional difficulty in designing a secure protocol lies in the application scenario that is going to protect, and how well it can handle different scenarios than the one it has been explicitly designed for.

Further our simulations show that ARAN it is an efficient as AODV in discovering and maintaining routes, at the cost of using larger routing packets which result in a higher overall routing load, and at the cost of higher latency in route discovery because of the cryptographic computation that must occur.

Reference:

[1] Hu, et. al. Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks MobiCom ’02.

[2] D. Bleichenbacher and A. May, “*New attacks on RSA with small CRTexponent in Public Key Cryptography*”, PKC 2006, volume 3968 of Lecture Notes in Computer Science, pages 1–13. Springer-Verlag, 2006.

[3] Bobba, et. al Bootstrapping Security Associations for Routing in Mobile Ad-Hoc Networks ISR TR 2002.

[4] D. Bleichenbacher and A. May, “New attacks on RSA with small secret CRT-exponents,” in *Public Key Cryptology—PKC 2006*, ser. Lecture Notes in Computer
Science. New York: Springer, 2006, vol. 3958, pp. 1–13.

[5] P. Papadimitratos and Z.J. Haas, ”Secure Routing for Mobile Ad Hoc Networks.” *SCS Comm. Networks and Distributed Systems Modeling and Simulation (CNDS2002)*, San Antonio, TX, Jan. 27-31, 2002

[6] Y. Wang, V. Giruka, and M. Singhal, “A fair distributed solution for selfish node problem in mobile ad hoc networks,” in proceedings of ADHOCNOW04, 2004.

[7] F. Kargl, A. Gei, S. Schlott, and M. Weber, “Secure dynamic source routing,” in proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS), 2005.

[8] H. Q, W. D, and K. P, “Sori: a secure and objective reputation-based incentive scheme for ad-hoc networks,” in proceedings of IEEE WCNC2004, March 2004.

[9] J. Kong et al. Providing robust and ubiquitous security support for mobile ad-hoc networks. In *Proc. IEEE ICNP*, pages 251–260, 2001.

[10] S.-J. Lee and M. Gerla. Split multipath routing with maximally disjoint paths in ad hoc networks.

[11] S. Murthy and J.J. Garcia-Lunca-Aceves. An efficient routing protocol for wireless networks. *ACM Mobile Networks and Applications Journal*, pages 183–197, Oct. 1996.

About Authors

V.Venkata Ramana obtained his Master’s degree in Computer Science Engineering and pursuing Ph.D degree in JNTUA, University and at present working as an Associate Professor in Department of Computer Science Engineering, SSITS, Rayachoti, Kadapa(Dist), A.P. His areas of interest include Software Architecture and Computer networking, data mining, and other latest trends in technology. He has more than 14 years of experience in teaching and research in the area of Computer Science and Engineering.

K.K.Basheer obtained his Master’s degree in Computer Science Engineering and pursuing Ph.D degree in JNTUA, University and at present working as an Associate Professor in Department of Computer Science Engineering, VITS, Rayachoti, Kadapa(Dist), A.P. His areas of interest include Network Security,IRS and Computer networking, data mining, and other latest trends in technology. He has more than 14 years of experience in teaching and research in the area of Computer Science and Engineering.

P.Srinivasa Rao obtained his Master’s degree in Computer Science Engineering and pursuing Ph.D degree in JNTUK, University and at present working as an Assistant Professor in Department of Computer Science Engineering, GMRIT, Rajam, Srikakulam(Dist) INDIA ,A.P. His areas of interest include Data mining ,IRS and Computer networking and other latest trends in technology. He has more than 05 years of experience in teaching and research in the area of Computer Science and Engineering.