ISSN:0975-9646

Secure Route Discovery in Wireless Image Content-Based authentication

SRINIVAS KOLLA, KIRAN
Department of computer science & engineering , Jawaharlal Nehru Technological University,Hyderabad

Abstract: The introduction of 3G wireless communication systems, together with the invasive distribution of digital images in mobile devices and the growing concern on their originality triggers an emergent need of authenticating images received by unreliable channels, such as public Internet and wireless networks. To meet this need, a content-based image authentication scheme that is suitable for an insecure network and robust to transmission errors. In proposed scheme,The 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 points of view. Recently, a security model tailored to the specific requirements of MANETs was introduced by Acs, Buttya´n, and Vajda.

INDEX TERMS— IMAGE CONTENT-BASED AUTHENTICITY VERIFICATION - WIRELESS IMAGE AUTHENTICATION - SECRET WAVELET FILTER PARAMETERIZATION - STRUCTURAL DIGITAL SIGNATURE (SDS), NETWORK PROTOCOLS: ROUTING PROTOCOLS (SECURITY),INFORMATION SYSTEMS (SECURITY), HIDDEN CHANNEL AND CONCURRENCY ATTACKS

1 INTRODUCTION

Recent advances in networking and digital media technologies have created a large number of networked multimedia applications. Those applications are often deployed in a distributed network environment that makes multimedia contents vulnerable to privacy and malicious attacks. For insecure environments, it is possible for an enemy to tamper with images during transmission. To guarantee trustworthiness, image authentication techniques have emerged to confirm content integrity and prevent forgery. These techniques are required to be robust against normal image processing and transmission errors, while being able to detect malevolent tampering on the image [1]. Such authentication techniques have wide applicability in law, commerce, journalism and national defence.

In the literatures, methods of image content authentication can be done by digital signature along appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. A digital signature (or crypto-hash) is a set of extracted features, which captures the essence of image content in compact representation [1]. It is stored as an extra file and later used for authentication. Signature based methods can work on both the integrity protection of the image and repudiation prevention of the sender.

The work extending the digital signature scheme from data (fragile or hard) authentication to content (semi-fragile or soft) authentication Discovery of routes is a major task. For image authentication, it is desired that the verification method be able to resist content preserving modifications while being sensitive to content changing modifications.

ROUTING is a basic functionality for multihop mobile ad hoc networks (MANETs). These networks are decentralized, with nodes acting both as hosts and as routers, forwarding packets for nodes that are not in transmission range of each other.Route discovery algorithms have been proposed in the literature. One of the advantages of the new approach—which we will refer as the ABV model—is that it highlights security issues related to concurrent protocol executions. Indeed, the authors of the ABV model prove that, within their model, the routing algorithms SRP [3] and Ariadne [13] are insecure and subject to a hidden channel attack. A solution is then proposed in the form of a novel route discovery algorithm, named endairA—the name reflects the fact that it applies security primitives in the reverse order of the Ariadne protocol—and a proof is also supplied for the claim that endairA is secure in the ABV model [13].

Our main contribution in this paper is to show that the security proof for endairA given in [15] is flawed and that this routing algorithm subject to a hidden channel attack in content-based image authentication over wireless channels. Revisiting the ABV model, we present several reasons why we think that concurrent security for MANET route discovery—i.e., the ABV model's security standard—is insufficient in practice, because it requires the absence of channels that are always present in any realworld MANET application. We then argue that a higher security standard—namely composability—is a fundamental requirement for ubiquitous applications. Subsequently, we make some observations about issues that have to be addressed by any routing protocol that achieves security in a composable model.

The organization of this paper is as follows: In Section 2, General framework of signature based image authentication scheme, which can be effected by hidden channel attacks and concurrency-based attacks over wireless environment and their weaknesses. In Section 3, we show that the security proof for endairA is flawed and that this algorithm is subject to a hidden channel attack. We then discuss the significance of concurrency-based attacks. This is followed in Section 4 by a general discussion on the requirements for a formal security framework for this.

2. GENERAL FRAMEWORK

Fig. 1 shows the brief diagram of a signature based image authentication scheme [1]. There are two main

problems in this diagram. One is that the scheme is effected by hidden channel attacks and concurrency-based attacks and the other is cause of some security problems as the publickey of reciver know to all.

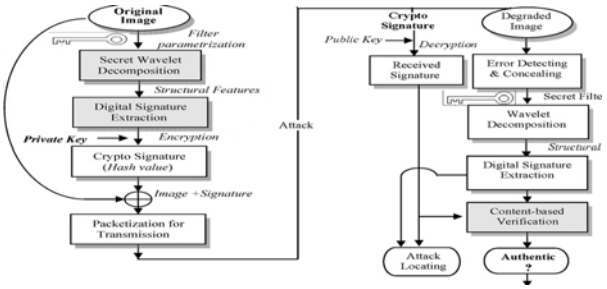

Fig. 1 diagram of a signature based image authentication scheme.

To tackle these problems while not sacrificing accuracy and increasing the complexity, a endairA routing algorithm is similarly subject to a hidden channel attacks and concurrency-based attacks.

A key problem in the construction of secure hash values is the selection of image features that are resistant to common transformations. When the features to represent its corresponding content are selected, one needs to consider not only its robustness to the acceptable manipulations but also its security (sensitivity) against malicious modifications. Actually, these two requirements are contradictive and application dependent. A typical approach is to extract image features that are invariant allowing content preserving image processing operations.

Some of the features that have been proposed in the literature include block-based histograms, image-edge information and the wavelet transforms [1]. However, since these features are publicly known, using such features alone makes the scheme susceptible to forgery attacks, even when the final hash is obtained by encrypting these features. Therefore the security mechanism should be combined into the feature extraction stage. Previous works mainly focused on the robustness study of features. The objective of this paper is to conduct an illustrative security study of features in order to improve the security of wireless image authentication systems without additional computational complexity by Secure Route Discovery.

3. THE PROTOCOL ENDAIRA

This is a variant of Ariadne, designed to address the hidden channel attack described above. In endairA, the route replies of intermediate nodes X_j are protected, rather than the route requests as in Ariadne. A typical route request broadcast by a node X_j , 0≤j≤p, on route $S = X_0, X_1, \ldots, X_p, X_{p+1} = T,$ is of the form $msg_{S,T,rreq} = (rreq, S, T, id, X_1, \ldots, X_j),$ while the route reply unicast by $X_j, 1 \leq j \leq p+1,$ is $msg_{S,T,rreq} = (rreq, S, T, id, X_1, \ldots, X_p, sig_T, \ldots, sig_{X_j}),$ where sig_{X_j} is the digital signature of X_j on the message field preceding it.

3.1 ANALYSIS OF ENDAIRA

The protocol endairA is claimed to be proven secure in the ABV security framework [13]. We now revisit the proof of security and identify a flaw. The proof in [13] considers the possibility of an attack against endairA being successful,
hoping to achieve a contradiction.

Let $(l_{ini}, l_1, \ldots, l_p, l_{tar})$ be some route that is accepted by endairA, where l_{ini} is the label of a nonadversarial initiator node and l_{tar} is the label of the target. This is assumed not to correspond to a valid route in the sense that it includes non-neighbor vertices. Since adversarial nodes can share labels, any number of adversarial nodes can be subsumed in a single label. However, Acs, Buttya´n, and Vajda exclude such faulty routes by subsuming all adjacent adversarial nodes, and indeed, any two adversarial nodes with direct means of communication (e.g., via out-of-band channels) as single nodes Consequently, adversarial nodes are, by definition, never adjacent in the ABV model. This is an arbitrary restriction that greatly limits the scope of the security statements in the ABV model in their ability to capture realistic security requirements. However, we do not need to leave this model to identify a problem with the security proof of endairA. So, for the sake of argument, we also assume that adversarial nodes are never adjacent. This implies that the route can be uniquely partitioned as follows: each partition consists of a single noncompromised identifier (label) or a sequence of consecutive compromised identifiers. A plausible route is one whose partitions correspond to that of a real route that physically exists in the network. The security statement of endairA is that it only accepts plausible routes. Note that this statement also does not consider an adversarial lengthening of a route by assignment of multiple labels to a single compromised network node as an attack. Again, this is a strong restriction on the security guarantees that the ABV model can provide, but we also follow this paradigm because we wish to show that endairA fails in the exact model in [13].

For the sake of seeking a contradiction, the proof in [13] lets $P_1, P_2, \ldots, P_k$ be a partition of $(l_{ini}, l_1, \ldots, l_p, l_{tar})$ which is a nonplausible route that has been accepted by endairA.This implies one of the two cases:

1) there exist two partitions $P_i = \{l_j\}$ and $P_{i+1} = \{l_{j+1}\}$ such that both l_j and l_{j+1} are identifiers that correspond to nonadversarial nodes that are not neighbors or 2) there exist three partitions $P_i = \{l_j\}, P_{i+1} = \{l_{j+1}, \dots, l_{j+q}\}$ and $P_{i+2} = \{l_{j+q+1}\}$ such that l_j and l_{j+q+1} are noncompromised identifiers and $l_{j+1}, \dots, l_{j+q}$ are compromised identifiers, but the nodes corresponding to l_j and l_{j+q+1} do not share a common adversarial neighbor. The flaw in the proof is the argument against the possibility of case 2. Quoting:

"Machine l_j must have received

$msg' = (rreq, l_{int}, l_{tar}, (l_1, \dots, l_p), (sig_{l_{tar}}, sig_{l_p}, \dots, sig_{l_{j+2}}))$

from an adversarial neighbor, say, A, since l_{j+1} is compromised. . . . . .

In order to generate msg' machine A must have received

$msg'' = (rreq, l_{int}, l_{tar}, (l_1, \dots, l_p), (sig_{l_{tar}}, sig_{l_p}, \dots, sig_{l_{j+q+2}}))$

because, by assumption, the adversary has not forged the signature of l_{j+q+1}, which is non-compromised. Since A has no adversarial neighbor, it could have received msg'' only from a non-adversarial machine. . . . . "

The fallacy with the above reasoning is contained in the last sentence: there is no such necessity for the adversarial node A to get information from a nonadversarial node. It is true that the ABV model prohibits direct communication (either via wireless links or through any out-of-band channels) between two adversarial nodes. However, there exist hidden channels available for compromised nodes to exploit and send communication through. For instance, compromised nodes can arbitrarily tamper with concurrent route discovery requests of endairA (which are not authenticated). These route requests need not be initiated by adversarial nodes (in compliance with an ABV model restriction), they just need to be initiated by honest nodes prompted by the adversary (through route discovery requests). Similarly, the requests do not need to be initiated dynamically (as the ABV model also restricts this), only to be underway concurrently and have their messages corrupted dynamically (in accordance with the ABV model).

I conclude that the proof makes the unwarranted assumption that no direct channels imply no direct bandwidth between adversarial nodes; the proof is therefore incomplete. It could be possible that the security claims remained valid even as their proof is incorrectly argued. However, we show that this is not the case. Indeed, in the next section, we give concrete examples of how to exploit hidden channels.

Fundamentally, endairA (and the ABV model) was developed to deal with a class of hidden channels, the intrinsic hidden channels of a wireless broadcast medium in a neighborhood. However, security is not achieved because other hidden channels remain present.

3.2 An Attack on endairA

This is a hidden channel attack that does not require out-of-band resources. Consider an instance of endairA with source node S and let

(S, A, X, B, Y, D, T)

be a sequence of identifiers of pairwise neighbor nodes in which only X, Y are faulty. In the attack, when the second faulty node Y receives $msg_{ST,rreq} = (rreq, S, T, id, A, X, B)$, it drops node B from the listing and transmits $msg_{ST,rreq} = (rreq, S, T, id, A, X, Y)$. Eventually, the route request will reach the target T, which will compute and send back a route reply. Node Y will then receive from D

$msg_{ST,rreq} = (rreq, S, T, id, A, X, Y, D, sig_T, sig_D)$

Now, Y can obviously attach its label and signature to this reply and transmit to B the extended reply, but B will not retransmit it because B is not included in the listing.However, suppose that Y had earlier received a request from D to find a route linking it to node A. Then, since the adversary schedules (nonadaptively) all the route discoveries prompted by honest nodes in the ABV model, it can arrange for this to be the case. Say the route request was $msg_{D,Arreq} = (rreq, D, A, id')$, with an identifier id'. Y mangles id' into some id'' that contains (possibly encrypted) information that X can use to reconstruct the signatures sig_T, sig_D in message (2) (and the signature sig_Y of Y if this is needed), before sending it along to B and eventually X. Now, the identifier id' will most likely not be long enough for this purpose, so node Y must take advantage of several route discovery requests that should go through Y to reach X, mangling all the identifiers. For example, Y may compute $\sigma(sig_T) || \sigma(sig_D) = id' || id'' || \dots || id^{(k)}$, where "||" is concatenation and σ is a bit permutation known to both X and Y, and use $id', id'', \dots, id^{(k)}$ as identifiers for route requests. Again, since the adversary can prompt honest nodes to create route discovery requests, it can ensure that enough sessions will have reached it ahead of

time (and nonadaptively). Eventually, X will be able to reconstruct these signatures and can then generate the route reply

$$msg_{STrreq} = (rreq, S, T, id, A, X, Y, D, sig_T, sig_D, sig_Y, sig_X)$$

which is sent back to the source S and validated.

Note that the route discovery sessions that were mangled by Y as part of the above attack will eventually be discarded by their respective initiators. Still, one route was accepted that is not plausible, violating the stated concurrent security of endairA. Moreover, the attack will succeed with overwhelming probability in those network topologies that contain a sufficient number of nonadversarial nodes (suitable for initiator and target of concurrent route discovery sessions).

The hidden channel used in this attack exploits the fact that there is enough redundancy in the protocol identifier id to hide signature information. Even for the version of endairA with no identifiers (insecure against replay attacks), the attack still applies because other hidden channels exist. For instance, the list of labels included in route requests may also be used to convey information. In particular, if there are n authorized labels, then there are $\binom{n}{k}$ possible lists of k labels that can be used to hide information. The node Y would mangle the concurrent requests by arbitrary combination of nodes to signal the appropriate information to X.

Digital signatures that use randomness (e.g., the DSA) can also be used to hide information [16]: the adversarial signer, instead of using a random string, uses the information to be transmitted. This information can then be extracted by any other adversarial node that knows the secret signing key (in our case, X must know the signingkey of Y).

3.3HiddenChannel and Concurrency Attacks

In all the attacks described above, including the attacks in [13], [17], adversarial nodes succeed in shortening plausible routes by removing intermediate nodes. The adversarial nodes use hidden channels to communicate and transfer the necessary data (signatures, etc.). The hidden channels that we considered above do not use out-of-band resources, although this is an obvious alternative.

However, there are other channels that in many respects are much more natural. Indeed, the main objective of a route discovery algorithm is to find a route that is a suitable communication channel. Route discovery per se makes little sense. It would, therefore, be natural for nodes to use for their communication a route that was discovered earlier, whatever their intention. Therefore, it is unreasonable to restrict nodes from using hidden channels. Note that privacy is a legitimate goal for secure communication, so intermediate nodes should expect to retransmit the encrypted data.

Let us now pursue our earlier discussion on interleaving protocol instances. In a networking environment, one should expect that several instantiations of a routing protocol are executed. Some may involve route discovery, while others route maintenance, data communication, or general network applications. It makes no sense to require that route communication can only start when all the other route discovery instantiations (and network applications) have been completed. Indeed, this argument should be carried to its logical extension: the security of any protocol should not be considered in isolation, but in the presence of concurrent executions, i.e., whether these involve the same protocol or other protocols. Consequently, in our adversarial model, we should allow the adversary to interleave instantiations of several protocols, all running concurrently.
This is a natural requirement for security.

4. THE UNIVERSAL FRAMEWORK FOR ROUTING ALGORITHMS

It is well known that attacks on ad hoc routing protocols can be very subtle. Attacks may exploit the nature of the wireless medium, the mobility of the system, power constraints, and more generally, the fact that the adversary is not necessarily bounded by the constraints on nonfaulty nodes (the system). It is important that such issues be taken into account when designing security models for wireless systems, and more generally, models for ubiquitous applications. The universal composability (UC) framework
[14] and the secure reactive systems model [18], [19] were designed to deal with the composition of concurrent protocol execution attacks, and are therefore, more appropriate models for ubiquitous applications. Obviously, one has to make allowances for the constraints imposed on ad hoc network systems and for the fact that their mobility may make conventional route discovery infeasible (e.g., when routes become disconnected by the time they are discovered4). Below, we list some important aspects that are often neglected in order to make security issues more manageable.

4.1 The Adversary

It is sometimes suggested that adversarial nodes should be bound by the same constraints as nonadversarial nodes, for example, have similar communication capabilities [12]. This may be the case for some applications, but it is not realistic. Although, it may seem reasonable to assume that the resources of adversarial nodes are (polynomially) bounded, allowing for the constraints on ubiquitous applications, it is unreasonable to assume that adversarial nodes cannot use more powerful transmitters than nonadversarial nodes, say transmitters that are 50 percent more powerful than the norm, if with such means they can compromise the system.

4.2 The Communication Medium

There are several rather nasty attacks on MANETs that are hard to prevent. Of these, the Sybil attack [20] and the wormhole attack are possibly the worst. The Sybil attack deals with problems caused by sharing secret identifying keys: although, a nonfaulty node is uniquely identified by its public keys, a faulty node may present itself as one of several nodes. In particular, a faulty node may present itself as several nodes during the neighbor discovery protocol. Unless there is some way of physically detecting the source of an identifying call, it is hard to detect such attacks.

In a wormhole attack, the adversary establishes an outof-band channel, or a system channel, to subvert the normal functioning of an ad hoc network. In the context of routing, this attack can be used to corrupt routing protocols.Wormhole attacks can be combined with timing or rushing attacks [21] in which the attacker succeeds in forwarding packets faster by using appropriate mechanisms or channels (possibly out-of-band). As with the Sybil attacks, these attacks are usually discounted as preventable at the network layer. It should be pointed out that claiming that an attack is easily preventable at the network layer is in many respects equivalent to claiming that the security of a wireless system can be achieved at the physical layer. Although, this may be the case for some restricted applications, yet it fails to take into account the malicious nature of some attacks. Note that route discovery is a distributed (global) computation, whereas neighbor discovery is a local process. Therefore, route discovery is better suited to identification of threats 4. In such cases, one may use one of the adaptive gossip protocols in [22]. such as the Sybil and wormhole attacks, which only become detectable when global information is collated.

4.3 Composability Issues

We argue that composability is an essential requirement for secure routing in MANETs. Indeed, MANETs can distinctly be characterized from fixed-infrastructure networks by the fact that both the control plane (routing messages) and the data plane (proper communication messages) are highly subject to a variety of attacks. It becomes essential to understand how the security requirements of each layer interfere with each other.

Indeed, interference between security properties at different layers also manifests itself in the fixed-infrastructure setting. We illustrate this point with a real-world example, the well-known rogue packet attack against SSL. In this active attack, a rushing node injects an SSL packet in an existing TCP connection, recomputing the TCP checksums to ensure acceptance of the inserted packet at the transport layer. When the SSL protocol daemon, residing at the session layer,6 receives the SSL packet (TCP payload), it determines that the packet has been tampered with by failing to verify the message authentication code (that the attacker is unable to forge for lacking knowledge of the shared authentication keys). The packet is therefore discarded at the SSL layer. This is because the TCP daemon has recorded that packet's sequence number as already received. The SSL session layer fails to recover the missing data, and therefore, SSL+TCP does not provide availability guarantees.

In this scheme, TCP provides availability but not integrity. SSL provides integrity but relies on the availability properties of TCP. This reliance proves unfounded, as the availability guarantees of TCP are only provided under the weaker integrity notion corresponding to verifiability of the TCP checksums. Composability fails accordingly.

MANET routing security presents very similar problems. Indeed, as has been demonstrated by the designers of the endairA protocol, even the provision of a single property (safety of routing discovery) requires at least a concurrent approach, as illustrated by the attacks on Ariadne [12]. We extend this observation by remarking that special care needs to be taken when assuming properties of lower network layers, especially when such properties are achieved under restrictions. If such restrictions are incompatible with requirements at other layers, a solution may be nominally composable but incomplete because no comprehensive solution is achieved (or achievable) in composition. As an example of such a shortcoming, we reexamine the endairA protocol.

In this protocol, safety-type properties (such as integrity) at the MANET control plane are achieved by assuming restricted availability of transmission channels. However, such restrictions may be fundamentally incompatible with liveness guarantees (such as availability) at the data (user) plane. For instance, an MANET could enforce that other forms of data transmission are interrupted while routing computations are ongoing, realizing the required restriction and supporting safety at the control plane. However, this strategy puts the liveness requirements of the control and data plane in direct conflict. Denial-of-service attacks against data transmission could be initiated by frequent triggering of new routing computations. Limiting the frequency of new routing computations might prevent such attacks at the expense of reducing the network capability to deal with frequent topology changes.

To summarize, in contrast with the situation for fixed infrastructure networks, where infrequency of topology changes can be assumed, and therefore, it may be acceptable to deny data services to destinations during any period where routing information to that destination is being (re)computed; in MANETs, it is not acceptable to assume temporal disjointness of the routing discovery and data communication phases, and security under composability of different protocols is necessary. It is insufficient to consider only the simpler (and yet hard to achieve) requirement of security under concurrent executions of the route discovery protocol.

5. CONCLUSION

A new security framework tailored for on-demand route discovery protocols in content-based image authentication over wireless channels. This represents a first effort toward a formal security model that can deal with concurrent attacks and is successful in mitigating a class of hidden channel attacks—the attacks that are intrinsic to the wireless broadcast medium in a neighborhood. However, as we observed above, there are a plethora of other hidden channels that become available through concurrent execution of route discovery protocols. Additionally, in the context of mobility, which requires that route discovery take place simultaneously with data communication, large additional bandwidth is naturally generated and available to adversarial nodes. Consequently, in the proposed formal model, it is impossible to prevent that adversarial nodes break up routes by inserting nonexisting links. To address this shortcoming, either more flexible definitions of routes must be employed (e.g.,redundant routing) or it becomes necessary to address global threats directly, such as those posed by Sybil,wormhole, and more generally, man-in-the-middle attacks. Further work will conduct more tests on the quality of degraded images.

REFERENCES

[1] LOU D.C., LIU J.L., LI C.-T.: 'Digital Signature-Based Image Authentication', in LU C.S. (EDS.): 'Multimedia security:steganography and digital watermarking techniques for protection of intellectual property' (Idea Group Inc., 2003)

[2] SEITZ J.: 'Digital watermarking for digital media' (Idea Group Publishing, 2005), Ch. 2

[3] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS '02), 2002.

[4] LU C.S.: 'On the security of structural information extraction/embedding for image authentication'. Proc.IEEE ISCAS'04, 2004, pp. 169–172

[5] GINESU G., GIUSTO D.D., ONALI T.: 'Mutual image based authentication framework with JPEG2000 in wireless environment', EURASIP J. Wirel. Commun. Netw., 2006, 2006, pp. 1–14 (Article ID 73685)

[6] SUN Q., YE S., LIN C.-Y.: 'A crypto signature scheme for image authentication over wireless channel', Int. J. Image Graph., 2005, 5, (1), pp. 1–14

[7] M.G. Zapata, "Secure Ad Hoc On-Demand Distance Vector Routing," Mobile Computing and Comm. Rev., vol. 6, no. 3,pp. 106-107, 2002.

[8] P. Papadimitratos and Z. Haas, "Securing Mobile Ad Hoc Networks," Handbook of Ad Hoc Wireless Networks, M. Ilyas, ed., CRC Press, 2002.

[9] YE S., SUN Q., CHANG EE-C.: 'Error resilient content based image authentication over wireless channel'. Proc. IEEE ICIP'06, 2006

[10] PETER M., UHL M.: 'Watermark security via wavelet filter parametrization'. Proc. Int. Conf. ICASSP, USA, 2000

[11] SWAMINATHAN A., MAO Y., WU M.: 'Robust and secure image hashing', IEEE Trans. Inf. Forensics Sec., 2006, 1, (2),pp. 215–229

[12] G. _ Acs, L. Buttya´n, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans.Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[13] G. _ Acs, L. Buttya´n, and I. Vajda, "Modelling Adversaries and Security Objectives for Routing Protocols in Wireless Sensor Networks," Proc. Workshop Security in Ad Hoc and Sensor Networks(SASN '06), pp. 49-58, 2006.

[14] R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols," Proc. IEEE Ann. Symp. Foundations of Computer Science (FOCS '01), pp. 136-145, 2001.

[15] BARROS J., RODRIGUES M.R.D.: 'Secrecy capacity of wireless channel'. Proc. IEEE Int. Symp. Information Theory,Seattle, USA, 2006

[16] G.Simmons, "The Subliminal Channels of the US Digital Signature Algorithm (DSA)," Proc. Third Symp. State and Progress of Research in Cryptography, pp. 35-54, 1993.

[17] L. Buttya´n and I. Vajda, "Towards Provable Security for Ad Hoc Routing Protocols," Proc. ACM Workshop Ad Hoc and Sensor Networks (SASN '04), 2004.

[18] B. Pfitzmann and M. Waidner, "Composition and Integrity Preservation of Secure Reactive Systems," Proc. ACM Conf. Computer and Comm. Security, pp. 245-254, 2000.

[19] B.P.M. Backes and M. Waidner, "A General Composition Theorem for Secure Reactive Systems," Proc. Theory of Cryptography Conf.(TCC '04), pp. 336-354, 2004.

[20] J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to-Peer Systems (IPTPS '02), pp. 252-260, 2002.

[21] Y.-C. Hu, A. Perrig, and D. Johnson, "A Survey of Secure Wireless Ad Hoc Routing Protocols," IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 28-39, May/June 2004.

[22] M. Burmester, T. van Le, and A. Yasinsac, "Adaptive Gossip Protocols: Managing Security and Redundancy in Dense Ad Hoc Networks," J. Ad Hoc Networks, vol. 5, no. 3, pp. 286-297, 2007.

AUTHOR PROFILE

SRINIVAS KOLLA obtained his Bachelor of Technology from Faculty of Computer Science and Engineering, Jawaharlal Nehru Technological University in 2009. Currently, he is doing master of Technology of Computer Science and Engineering, Jawaharlal Nehru Technological University .His main research areas include computer security, information security,mobile computing and computer networks.