A Survey on Formal Modelling for Secure Routing in Mobile Ad hoc Networks

Parul Yadav
Department of Computer Science and Engineering
Institute of Engineering and Technology
Lucknow - U.P., India

Manish Gaur
Department of Computer Science and Engineering
Institute of Engineering and Technology
Lucknow - U.P., India

ABSTRACT
Mobile ad hoc network is an autonomous collection of mobile or stationary nodes communicating with each other via radio transceivers that has limited radio transmission range. In ad hoc networking, nodes are connected without any fixed infrastructure. Applications for mobile ad hoc network range from personal networks to emergency services. Major challenges to these innovative networks are due to highly dynamic topology and limitation of resources like battery power & bandwidth.

Security of routing protocols is one of the crucial and emerging issues in mobile ad hoc networks. A lot of secure versions of routing protocols in mobile ad hoc networks are already been proposed by eminent researchers. But most of them are tested by means of simulation. Simulation techniques have its limitations as it can only find presence of error rather than absence of error. To overcome this situation, formal methods are used that can verify systems using theorem proving or automated model checking techniques. This paper presents a survey on research done, so far, in line of formal modelling for secure routing in mobile ad hoc networks. The novelty of this paper is to highlight key features of proposed models for MANETs and open an area for future research.

General Terms
Formal modelling, mobile ad hoc network Algorithms

Keywords
Survey on MANETs algebra, calculus for MANETs, secure routing protocols

1. INTRODUCTION
Mobile ad hoc network (MANET), an infrastructureless wireless network, is the ultimate frontier in wireless communication. In mobile ad hoc network, nodes communicate over relatively bandwidth constrained wireless links. Nodes can form and de-form the network on the-fly without any system administration. Applications for mobile ad hoc network includes emergency disaster relief, military operations, community networking and interaction between attendees at a meeting etc.. Additionally, dynamic topology, multi hop, large network size along with device heterogeneity [1], battery power and bandwidth constrain make the design of adequate routing protocols a major challenge.

Mobile ad hoc network allows nodes to communicate with each other via radio transceivers that have limited radio transmission range. Therefore, packets to distant recipients are required to be routed through some intermediate nodes. Each node functions as end node and router. Routing protocols [2] for mobile ad hoc networks can be classified in three major categories: on-demand, proactive and hybrid. This paper briefs routing protocols for MANETs along with list of some existing secured versions of routing protocols.

Security attack in mobile ad hoc networks is also a one of the challenging and emerging issues [3]. Attacks can be classified according to their origin or their nature. Based on the origin, attacks are divided into two categories, external and internal [4]. On the basis of operation of the network, attacks in mobile ad hoc networks are categorized as active and passive attacks. Besides it, routing attacks are also classified into five categories: attacks using impersonation, modification, fabrication, replay, and denial of service (DoS). Security of routing protocols for mobile ad Hoc networks is an active area of research [3].

The challenge of MANETs is to design and verify robust routing protocol with adequate security schemes for these innovative networks. This paper describes importance of verification for MANETs. Most of the proposed routing protocols are employed to be verified using simulations and live testing [5]. Simulation and testing are not sufficient to verify design flaws or subtle errors left in a protocol. In order to achieve this goal, formal methods based approaches will be needed. Formal methods establish proof of correctness. However, it is a challenge to formally model basic characteristics of mobile ad hoc networks such as node mobility, dynamic topology & node connectivity and other necessary aspects like routing & security features. In this paper, strengths and properties of various proposed formal models for MANETs are brought to light and scope for further research is suggested that may provide researchers with new dimensions for research.

This paper is organized in five sections. Section 2 briefly presents summary of routing protocols in mobile ad hoc network. Section 3 is a short description of verification of MANETs. Section 4 presents formal modelling for MANETs. Section 5 sums up conclusion & future scope of this survey.

2. ROUTING PROTOCOLS IN MOBILE AD HOC NETWORKS
Routing protocols provide rules to decide route from source to destination to deliver packets. Based on the mechanism of routing information update, routing protocols in mobile ad hoc networks can be broadly classified into three categories. Three major categories of routing protocols [2] for mobile ad hoc networks are: on-demand (reactive), table-driven (proactive) and hybrid.

Reactive routing protocols [2] establish the necessary route whenever it is needed, by initiating a route discovery process. They use less bandwidth to maintain the network topology information in routing tables at each node and do not require unnecessary periodic updates of routing information. Some examples of reactive routing protocol are: AODV (Ad Hoc

On-Demand Distance Vector Routing), DSR (Dynamic Source Routing), LMR (Lightweight Mobile Routing), CBRP (Cluster Based Routing Protocol), and TORA (Temporary Ordered Routing Algorithm). Some secure versions of DSR, reactive routing protocol, are QoS Guided Route Discovery [6], Securing Quality of Service Route Discovery, Ariadne [7] and CONFIDANT [8]. AODV also has its secure versions such as CORE, SAODV and SAR [9]. Some other secure versions of reactive routing protocols are SPREAD and ARAN.

In proactive routing protocols [2], every node maintains the information about the other nodes in the network in routing table. Routing tables are updated by periodically flooding routing information in the whole network. Whenever a route from source to destination is required, source node runs an appropriate routing algorithm on the basis of information in routing table it maintains. Examples of proactive routing protocol are: DSDV (The Destination Sequenced Distance Vector Routing Protocol), CGSR (Clusterhead Gateway Switch Routing), WRP (Wireless Routing Protocol) and OLSR. Secure Efficient Ad hoc Distance vector (SEAD) [10] is based on DSDV and designed mainly to overcome security attacks such as DoS and resource consumption attacks. SLSP (secure link state protocol) [11], is a secure version of OLSR which uses digital signature and one-way hash chains to ensure the security of link-state updates.

Hybrid routing protocols [2] take advantages of both reactive and proactive routing protocols. For example, proactive routing protocol can be used for a node communicates with its neighbors, and reactive routing protocol can be used with nodes that are farther away from the node. In hybrid routing protocol, nodes within certain geographical area use proactive routing protocols while outside the geographical area use reactive routing protocols. ZRP (Zone Routing Protocol), ZHLS (Zone-based Hierarchical Link State routing) and HARP (Hybrid Ad hoc Routing Protocol) are examples for hybrid routing protocols in mobile ad hoc networks. SRP is based on ZRP.

Routing protocols in mobile ad hoc network are required to be verified for their correctness.

3. VERIFICATION OF MANETS

Verification of designed model for MANETs is important to proof its correctness. Most of the routing protocols in mobile ah hoc networks are tested by simulation tools. The simulation-based testing has three shortcomings:

1. scenario specific results
2. limited scalability of simulation tools
3. slowing down the protocol engineering cycle due to large simulation time.

Thus, by simulation [5] these systems can not be verified by exploring all conditions related to them. On the other hand, formal methods can be used to model routing protocols in mobile ad hoc networks, and then verify them using theorem prover or (semi) automated model checking techniques.

Formal methods model complex systems as mathematical entities. By modelling a complex system using formal methods, the properties of the system can be verified in a more thorough fashion than testing it using simulation. Formal design basically has three steps: formal specification, verification and implementation. Formal modelling for routing protocols in mobile ad hoc networks is difficult due to its challenges like dynamic topology, diverse flooding patterns. A brief description to formal modelling for MANETs is given in next section.

4. FORMAL MODELLING FOR MANETS

Formal methods are techniques used to model complex systems as mathematical entities. Formal verification of security protocols is of particular importance, since flaws have been found in many published protocols. Flaws are sometimes overlooked during scrutiny due to the imprecise, informal manner in which these protocols are specified and frequently remain undiscovered for years. Much effort has therefore been spent in developing and applying theory for formal verification of security protocols. Several formal methods for automated verification of security protocols already exist. However, few of them are applicable to security protocols for mobile ad hoc networks. Some of the existing formal models for MANETs are briefed below:

4.1 Calculus of Mobile ad hoc Networks

[12] presents a value passing process calculus called as Calculus of Mobile Ad hoc Networks (CMN) written in CCS style that can not be used to transmit channel names. CMN gives a behavioural theory to formally prove some of the properties of mobile ad hoc network such as ubiquity of mobile nodes, observation for silent nodes, mixing up infinite output sequences, obfuscating message transmission, range repeaters, range repeaters with two channels, saving antenna power. CMN allows nodes to run in parallel and uses channel that can be private or public to broadcast messages. A typical node in CMN looks like $n[P]_{l,r}^{\mu}$. Each node is assigned with network address n, physical location l, transmission range r, mobility tag μ to define it as mobile or stationary and executing process P. CMN represents connectivity of node by location l and transmission radius r. Distance between two nodes is calculated using distance function $d(.,.)$ that takes locations of the two nodes as input and returns their distance as output. Operational semantics is given in terms of reduction semantics and labelled transition system (LTS) that concide each other. LTS has rules for processes and networks both. It has incorporated the rule for message loss and unobservable local activity of the network. It has modelled the situation in which potential receiver do not receive broadcast message.

In this paper, node can not derive its transmission range and physical location due absence of support for GPS. It does not support arbitrary connections and disconnections of nodes. It has absence of rules for multicast and unicast communication. In this paper, the presence of specific protocol e.g., CSMA/CA is assumed to avoid collisions. When a node is moving, it can not do any other action that is undesirable for these innovative networks. Lacking of scope extrusion restricts to transmit channels. This calculus does not support concept of store to record routing table, node failure and security.

4.2 BUM Calculus

[13] presents a process calculus to analyze and model properties of mobile ad hoc network along with its routing protocols. In this paper, a formal model for cost effective routing protocol is developed. Cost effectiveness is achieved by taking energy efficiency of nodes into account. In mobile

ad hoc networks, nodes are highly dynamic and with limited battery power. Drain of battery power at any node affects the abilities of node itself e.g., to forward packets on behalf of other nodes and finally results in reduction in overall lifetime of the network. This process calculus that is an extension of CMN[12], named as BUM calculus, supports local broadcast, multicast and unicast communications as well. Output action is attached with list of intended recipients of the message to ensure unicast and multicast communication. Connectivity of nodes is maintained by location and transmission radius. Each node has a location, transmission radius, logical location, physical location, mobility tag to denote stationary or mobile node. To check whether two nodes are in transmission range of each other, Distance function is calculated. Message transmitted will only be received by the nodes which lie in the transmission range of each other. Nodes can adjust their transmission radius and even turn off to save power.

This paper does not specify how to maintain routing table at nodes. It does not ensure secure routing.

4.3 Restricted Broadcast Process Theory

[14] introduces a new process algebra to model essential modelling concepts of MANETs along with its routing protocols. It supports lossy local broadcast, connectivity and connectivity changes. Connectivity description and network specifications are modelled separately. Connectivity is modelled implicitly by a topology invariant. Topology invariant defines a set of possible topologies that quantify a state. Topology changes are also modelled implicitly in the semantics.

In this paper, only one channel for MAC layer is considered. Therefore, at any time only one node can get the channel and broadcast. Security aspect is yet to be incorporated here.

4.4 Routing Process Algebra

[15] presents a process algebra to model and verify routing protocols in mobile ad hoc networks. The main properties of MANETs that are considered in this paper are local broadcast, connectivity and topology changes. Connectivity is modelled using connectivity function. Mobility is implemented implicitly in semantics by imposing restriction in form of pre-condition over connectivity function in each transition. These pre-conditions define possible movements among nodes. An application of this model is illustrated on cluster formation process in cluster based routing protocol.

This model is not verified using network simulation or bisimulation. Future scope also includes designing and implementation of an automated tool for formal analysis of the networks.

4.5 ω Calculus

[16] presents a process calculus named as ω calculus to model mobile ad hoc networks and its protocols. It has modelled key features of nodes i.e., to broadcast message to nodes that are in its transmission range and to dynamically move within the network. ω calculus separates communication and computational behaviour of nodes from its physical transmission range. Local broadcast is modelled using group based support.

Future work involves implementation of optimizing compiler and compositional model checker like CCS for ω calculus. Implementation of compilation techniques for broadcast and multicast communication is yet to be done. ω calculus supports bidirectional connectivity that can be further extended for unidirectional node connections.

4.6 CBS$^{\#}$ Calculus

[17] presents a model for formal analysis of secure mobile ad hoc network. It emphasizes local broadcast by which only adjacent nodes of the sending node can receive a transmitted message. It includes separation of process connectivity and process actions. Connectivity is determined by node movement rather than process actions. Connectivity in the midst of nodes or adjacent nodes is explicitly modelled using connectivity graph. In this paper, notion of private store is used to model routing tables. Routing tables are updated only after receiving packets from authorized node of the network that are identified using public key digital signature approach.

The work can be extended for multiple attackers or hierarchy of attackers. Proofs of some more properties of MANETs also have scope for modelling. Connectivity graph can be abstracted by directed and weighted graphs.

4.7 E-BUM Calculus

[18] presents a process calculus named as E-BUM calculus, an energy aware calculus for broadcast, unicast and multicast communications for MANETs. Energy conservation is an important issue as mobile nodes are powered by limited battery power. Unicast and multicast communications save power and bandwidth and reduce error rate. Energy efficiency is achieved by reducing power consumption of node. Power consumption of nodes can be reduced by adjusting transmission range of the nodes. The ultimate goal is to maintain trade-off between network connectivity and power saving. It supports local broadcast, arbitrary connections and disconnections of nodes. It formalizes two different notion of interferences i.e. sender centred interference and receiver centred interference. It verifies the absence of interference between a specific set of nodes. Each node is associated with its logical location, physical location, executing process, maximum transmission range, distance covered in one computational step. Distance between two nodes is calculated using distance function $d(.,.)$. Nodes can be mobile or stationary. It explains the calculus using an example considering emergency due to earthquake where communication is required to be maintained among ambulances. It has proved some properties of ad hoc network e.g., silent nodes can not be observed, simulation of stationary nodes, range repeaters.

In this paper, it is assumed that transmission power is considered based on information given by communication protocol. At the time of movement, nodes can not do any other action.

4.8 Framework for Secrecy Properties of MANETs

[19] presents a framework to automatically verify security aspects of routing protocols in MANETs. It is an extension of [17], [20]. It gives syntax for distributed applied pi calculus with broadcast and procedure to generate Horn clauses. Public key digital signature scheme is used to provide security which is further verified for ARAN protocol. It does not ensure security against internal attacks.

4.9 Automatized Verification of ad hoc Routing Protocols

[21] performs model checking of routing protocols in mobile ad hoc networks. It uses SPIN and UPPAAL model checking tools to verify LUNAR (Lightweight Underlay Network Ad hoc Routing Protocol) as it is less complex compared to other routing protocols in mobile ad hoc network. It highlights the most fundamental errors like failure to route correctly and problems in operation like routing loops. It focuses also on timing considerations to react with topology changes. Existing path between two nodes is defined with respect to time too. Valid path excludes possibility of routing loops. LUNAR is a reactive ad hoc routing protocol that is verified by SPIN and UPPAAL model checking tools. Data and control aspects of LUMAR are verified through SPIN. UPPAAL is used to verify the timing requirements of LUNAR.

For verification number of nodes, nature of topology, scenarios are assumed to be limited in order to overcome state space storage overhead. These model checking tools also involve manual consideration and require to be more automatic. Automation approach can be extended for infinite-state verification and needs to cover all possible topologies for any number of nodes. For verification theorem proving method can then be used.

4.10 BAN Logic to Model Routing Protocol for MANETs

[22] presents BAN logic to formalize routing protocols in MANETs. It verifies security and authentication of routing protocol taking example of Authenticated Routing for Ad hoc Networks (ARAN). In order to analyze a protocol, it expresses assumptions, goals and steps of protocol as formulas in a symbolic notation. It also applies a set of deduction rules called postulates. Novelty on this paper includes uncovering the weak point of redundancies that results in reduction in computing overhead of battery limited mobile nodes.

4.11 Verification of MANET using HLPSL and AVISPA

[23] models and verifies the security properties of implicit on-demand routing protocols using model checking tools HLPSL and AVISPA that provide relatively higher degree of automation than any other automation tools like SPIN.

4.12 Formal Analysis of Privacy Properties for Routing Protocols

[24] presents a framework for formally analyzing privacy properties for routing protocols in MANETs. This calculus, usable for large class of routing protocols, is a variant of applied π calculus [25] and inspired from some other calculi (e.g. [17, 26, 27]). It models basic features of routing protocols e.g., topology of the network, broadcast communication, internal states of nodes etc., privacy properties chiefly, indistinguishability, unlinkability, anonymity. Indistinguishability deals with the possibility to distinguish some external actions undertaken by an agent from another. Unlinkability is related to the ability for an attacker to link certain actions together. Anonymity concerns the disclosure of information such as the identity of the sender, or the identity of the receiver. These properties are formalized using a notion of equivalence between traces. The formalization of these properties is applied on two versions of ANODR routing protocol [28]. It considers an eavesdropper who listens to some nodes of the network or even all of them. Basically, an eavesdropper can see messages that are sent from locations he is spying on, and can only encrypt, decrypt, sign messages or perform other cryptographic operations if he has the relevant keys.

Cryptographic primitives such as encryption, signature, and hash function, are represented by function symbols Σ. To model algebraic properties of cryptographic primitives, it defines an equational theory by a finite set E of equations. The framework models the intented behaviour of node(s) by a process. The syntax for process involves sending messages, receiving messages, no action, conditional activity, reading with condition in routing table, writing to routing table, parallel activity, replication, fresh name creation.

It does not consider an active attacker who controls the entire network. It can be modelled for more general model of protocols to represent high-level operations in routing protocols (e.g. reversing a list). Another direction is the enrichment of this attacker model, so as to model fully compromised nodes which disclose their long-term keys or fresh nonces generated during the execution of the protocols, and active attackers able to forge messages and interact with honest agents.

4.13 Attack Model for SRP Routing Protocol

In this paper [29], the security of routing protocol in MANETs is analyzed using Spi calculus and abstract interpretation. Spi calculus is an extension of π calculus with basic cryptographic theorem where private information can be sent and received by the processes over public channels in a secure manner. It describes and analyzes SRP(Secure Routing Protocol). It proposes the denotational semantics for the Spi calculus. It is an extension of Stark's predomain equations [30] for the π calculus. The extension can manage complexity in data structures and possibility of extruding multiple names through these structures. It covers predomains for input action, output action, public-key ciphertexts, secret-key ciphertexts , digital signatures. The attack process model, based on the model presented in DOLEV-YAO [31], describes general attacker in cryptographic protocols. The result shows the weaknesses of SRP in view of attack process model. It proves that security properties can not be ensured by using only Message Authentication Code (MAC) and Security Association (SA) in SRP. The basic reason of the SRP's flaw is that the intermediate nodes can not be guaranteed to be the trusted nodes due absence of any corresponding mechanism.

It does not provide a secure model rather proposes a attack model to analyze the flaws of SRP. This calculus can be extended to other cryptographic features to reveal some unknown flaws and test other secure protocols.

4.14 Formal Verification using SPIN Model Checker

[32] verifies ad hoc routing protocols using a model checker SPIN [33], a generic verification system that supports design and verification of asynchronous process systems and accepts design specifications written in verification language PROMELA. It implements add-ons like broadcast system, timers, mobility in SPIN to model ad hoc routing protocols. It performs verification of 5-node model of Wireless adaptive routing protocol (WARP). It verifies route discovery mechanism of WARP.

Security verification still has scope for verification using SPIN model checker.

4.15 Framework for Service Discovery Protocols in MANETs

[34] has proposed a framework to provide a formal basis for performance evaluation and behavioral study of service discovery protocols in mobile ad hoc networks. It evaluates various service discovery architectures against a given set of metrics. It provides a generic approach to specify protocols and an automated process for performance evaluation and behavioral study.

4.16 Nomad

[35] is a well adapted formal language called Nomad. In this paper, an analysis is performed using dedicated algorithms that allow checking the collected trace against a set of functional and security properties specified in the language.

4.17 Graph and Net Technologies for Formal Modelling and analysis of MANETs

[36] presents an appropriate integration of Petri nets, graph transformation concepts and algebraic specification techniques for formal modelling and analysis of flexible processes in mobile ad hoc networks. It yields low level and high level Petri net transformations [37, 38] using net transformation rules to adapt the net structure to changing requirements of the system.

4.18 Model based on Game Theory

[39] has developed a model based on game theory. The model formally explains basic characteristics of ad hoc networks e.g., nodes' selfishness, network mobility etc.. It covers strategies for cooperation to formally study and analyze. e.g., it describes a simple strategy that enforces packet forwarding among nodes. In this paper, the proposed approach is a cooperation based on Bayesian games, where the players are the nodes in the network.

4.19 BeeAdHoc MANET Routing Protocol

[40] presents a mathematical model for BeeAdHoc MANET routing protocol. BeeAdHoc model includes routing overhead, route optimality and two key performance metrics for BeeAdHoc MANET routing protocol. The collision model at MAC layer is one of the key features of BeeAdHoc model. The mathematical expressions of the performance metrics ensure the behavior of this routing protocol without resorting to scenario specific time consuming simulations.

4.20 Routing Algorithm based on Reinforcement Learning

[41] has proposed a new routing algorithm based on reinforcement learning. Due to dynamic nature of nodes in mobile ad hoc networks, existing routing protocols like AODV, DSR do not ensure all the challenges of the network. In this paper, the performance of Q-Routing is optimized by the generalization of prioritized sweeping. Here, the system is formally modelled as a distributed optimization problem and verified mathematically for its correctness.

Based on this survey, we sum up that basic features of MANETs are modelled and may secure routing in ad hoc networks in presence of external attacks. But models proposed in [23, 34, 35, 36, 39, 40, 41] etc. can not formally verify routing protocols against internal attacks in MANETs.

5. CONCLUSION AND FUTURE SCOPE

Designing of secure routing protocols is one of the key issues in MANETs. Various secure routing protocols have been proposed in [6, 7, 8, 9, 10, 11]. Most of these, verified using simulation tools, still has flaws. The simulation-tools have certain limitations like scenario specific results, limited scalability. Thus, simulation tool [5] can not be used to verify these systems by exploring all conditions related to them. On the other hand, using formal methods, these systems can be modelled, and then verified using theorem prover or (semi) automated model checking techniques. This survey has presented key features of various proposed formal models for MANETs. [19, 23, 24, 29, 35] provide formal frameworks to verify security aspects in MANETs.

Researchers have contributed by modelling basic properties like node mobility, local broadcast and dynamic topology etc. of MANETs and public key cryptography mechanism for secure routing in MANETs that can secure route discovery mechanism in presence of external attackers.

In MANETs, there can be internal attackers that can silently disturb the normal functionally of routing protocols and can consume limited resources. When faced with internal attacks, a secure protocol must continue to meet its goals. In our future work, we intend to design and verify a detection model for internal attackers for smooth functionally of routing protocols. The goal of our detection model will be to provide accurate, reliable, secure, loop free, energy efficient route that is always available. We will focus on a framework for the formal verification of secure MANET routing protocols with respect to their stated security goals. Our aim will be to design a systematic approach for secure ad hoc network routing protocol.

6. REFERENCES

[1] Thomas Plagemann, Vera Goebel, Carsten Griwodz, and Pål Halvorsen, Towards Middleware Services for Mobile Ad-hoc Network Applications, IEEE Workshop on Future Trends of Distributed Computing Systems, pp. 249-255, 2003

[2] Changling Liu and Jörg Kaiser, A Survey of Mobile Ad Hoc network Routing Protocols, Tech.Report Series, Nr. 2003-08, University of Magdeburg, pp. 1-37, 2005

[3] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang, Security In Mobile Ad Hoc Networks: Challenges And Solutions IEEE Wireless Communications, vol. 11, issue 1, pp. 38-47, 2004

[4] D. Djenouri, L. Khelladi, and N. Badache, " A survey of security issues in mobile ad hoc and sensor networks, IEEE Commun. Surveys Tutorials, vol. 7, pp. 2-28, 2005

[5] Henrik Lundgren, Implementation and Real-world Evaluation of Routing Protocols for Wireless Ad hoc Networks , Licentiate thesis, Uppsala University, 2002.

[6] W. Liu and Y. Fang, SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks, Proc. IEEE INFOCOM, vol. 4, pp. 2404-2413, 2004

[7] Y. Hu, A. Perrig, and D. B. Johnson, Packet Leashes: A defense against Wormhole Attacks in Wireless Ad Hoc Networks, Proc. IEEE INFOCOM 2003, vol. 3, pp. 1976-86, 2003

[8] S. Buchegger and J. L. Boudec, Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes-Fairness In Dynamic Ad-hoc Networks), Proc. IEEE/ACM Symp. Mobile Ad Hoc Networking and Computing (MobiHOC), pp. 226-236, 2002

[9] Y. Wang, G. Attebury, and B. Ramamurthy, A Survey of Security Issues in Wireless Sensor Networks, IEEE Commun. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, 2006

[10] Y. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, IEEE Comp. Society, vol. 2, issue 3, pp. 28-39, 2004

[11] Y. Hu and D. B. Johonson, Securing Quality-of-Service Route Discovery in On-Demand Routing for Ad Hoc Networks, Proc. ACM SASN '04, pp. 106-117, 2004

[12] Massimo Merro, An Observational Theory for Mobile Ad Hoc Networks (full version), Information and Computation, vol. 207, issue 2, pp. 194-208, 2009

[13] Lucia Gallina, Sabina Rossi, A Model for Broadcast, Unicast and Multicast Communications of Mobile Ad Hoc Networks available http://www.dsi.unive.it/ srossi/Papers/icmsc10.pdf

[14] Fatemeh Ghassemi, Wan Fokkink, Ali Movaghar Restricted Broadcast Process Theory, Proc. IEEE SEFM 08, pp. 345-354, 2008

[15] Fatemeh Ghassemi, Ali Movaghar, Formal Modeling Routing Protocols in Mobile Adhoc Networks, The CSI Journal on Comp. Sci. And Engg., Vol. 5, No. 2& 4(b), p 46-55, 2007

[16] Anu Singh, C. R. Ramakrishnan, Scott A. Smolka, A Process Calculus for Mobile Adhoc Networks, Sci. Comput. Program., vol. 75, issue 6, pp. 440-469, 2010

[17] Sebastian Nanz, Chris Hankin, A Framework for Security Analysis of Mobile Ad Hoc Networks, Electronic Notes in Theor. Comp. Sci., vol.367, issue 1, pp. 203-227,2006

[18] Lucia Gallina, Sabina Rossi, A Process Calculus for Energy-Aware Multicast Communications of Mobile Adhoc Networks , Wireless Communications and Mobile Computing, pp. 1-16, 2012

[19] Hans Huttel, Willard Thor Rafnsson, Secrecy in Mobile Adhoc Networks available http://www.cse.chalmers.se/ rafnsson/article.pdf

[20] Martin Abadi, Bruno Blanchet, Analyzing Security Protocols with Secrecy Types and Logic Program, Journal of the ACM 52,pp. 102-146, 2005

[21] Oskar Wibling,Joachim Parrow, Arnold Pears, Automatized Verification of Adhoc Rouitng Protocols

[22] Qiuna Niu, Formal Analysis of Secure Routing Protocol for Ad hoc Networks , Proc. IEEE WCSP 09, pp. 1-4, 2009

[23] Mihai-Lica Pura, Victor-Valeriu Patriciu, Ion Bica, Modeling and formal verification of implicit ondemand secure ad hoc routing protocols in HLPSL and AVISPA, International Journal of Computers and Communications, Issue 2, Volume 3, pp. 25-32, 2009

[24] Remy Chretien, Stephanie Delaune, Formal analysis of privacy for routing protocols in mobile ad hoc networks,Proc. ACM POST'13, pp. 1-20, 2013

[25] M. Abadi, C. Fournet, Mobile values, new names, and secure communication, In Proc. 28th Symposium on Principles of Programming Languages (POPL'01), pp 104-115. ACM Press, 2001

[26] M. Arnaud, V. Cortier, S. Delaune Modeling and verifying ad hoc routing protocols, In Proc. 23rd IEEE Comp. Security Foundations Symposium (CSF'10), pp 59-74, IEEE Comp. Society Press,2010

[27] V. Cortier, J. Degrieck, S. Delaune Analysing routing protocols: four nodes topologies are sufficient, In Proc. of the 1st International Conference on Principles of Security and Trust (POST'12), LNCS, pp 30-50. Springer, 2012.

[28] J. Kong, X. Hong, ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks, In Proc. 4th ACM Interational Symposium on Mobile Ad Hoc Networking and Computing, (MobiHoc'03), ACM, 2003

[29] Xu Donghong1, Jiang Shujuan,Qi Yong, Security Properties Analysis of Routing Protocol for MANET ,Second International Conference on Networks Security, Wireless Communications and Trusted Computing, pp 405-408, IEEE Comp. Society Press, 2010

[30] Matthew Hennessy, A fully abstract denotational semantics for the pi calculus , Theoretical Comp. Sci., 278(1–2),pp.53–89, 2002

[31] V.Cortier,H.Comon,et al, Deciding Security properties for cryptographic protocols, Application to key cycles, ACM Transactions on Computational Logic, pp. 1-39, 2009

[32] R. de Renesse, A. H. Aghvami, Formal verification ad hoc routing protocols using SPIN model checker, IEEE MELECON 2004, pp. 1177-1182, 2004

[33] G. J. Holzmann, The model checker SPIN , IEEE Transactions on Software Engineering, vol. 23, No. 5, pp. 279-295, 1997

[34] Avinash Shenoi, Yelena Yesha, Yaacov Yesha and Anupam Joshi, A Framework For Specification And Performance Evaluation Of Service Discovery Protocols In Mobile Ad-Hoc Networks , Ad Hoc Networks, Volume 4 Issue 1, pp. 1-23, 2006

[35] Wissam Mallouli, Bachar Wehbi, Ana Cavalli and Stéphane Maag, Formal Supervision of Mobile Ad hoc Networks for Security Flaws Detection , Book chapter in Security Engineering Techniques and Solutions for Information Systems: Management and Implementation, Information Science Reference - IGI Global. ISBN: 9781615208036, 2011

[36] Kathrin Hoffmann, Formal Modeling and Analysis of Mobile Ad Hoc Networks and Communication Based Systems using Graph and Net Technologies , Bulletin of The EATCS no 101, pp 148-160, 2010

[37] H. Ehrig, K. Hoffmann, J. Padberg, C. Ermel, U. Prange, E. Biermann, and T. Modica. Petri net transformations, In Petri Net Theory and Applications, pp. 1-16, I-Tech Education and Publication, 2008

[38] H. Ehrig, K. Ehrig, U. Prange, and G. Taentzer, Fundamentals of Algebraic Graph Transformation, EATCS Monographs in Theoretical Comp. Sci., Springer Verlag, 2006

[39] A. Urpi, M. Bonuccelli, S. Giordano, Modelling cooperation in mobile ad hoc networks: a formal description of selfishness, available ftp://ftp-sop.inria.fr/maestro/WiOpt03PDFfiles/urpi10.pdf

[40] Muhammad Saleem, Syed Ali Khayam, Muddassar Farooq, Formal Modeling of BeeAdHoc: a Bio-inspired Mobile Ad Hoc Network Routing Protocol, In: ANTS conference, LNCS 5217, pp 315-322, Springer-Verlag Berlin Heidelberg, 2008

[41] Shrirang Ambaji Kulkarni1, Dr. G Raghavendra Rao, Formal Modeling of Reinforcement Learning Algorithms Applied for Mobile Ad Hoc Network,International Journal of Recent Trends in Engineering, Vol 2, No.3, pp 43-47, 2009