International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Present State of the Art of Intrusion Detection Systems in MANETs: Finding Research Gaps

V. L. Pavani[1], Prof. B. Sathyanarayana[2]

[1]Research Scholar, Department Computer Science and Technology,
Sri Krishnadevaraya University, Anantapur-515004, Andhra Pradesh, India

[2]Chairman, Department of Computer Science and Technology,
Sri Krishnadevaraya University, Anantapur-515004, Andhra Pradesh, India

Abstract: ***MANET is network with mobile nodes which has no fixed infrastructure support. As the nodes are energy-constrained and have mobility in the real world, they are vulnerable to various kinds of attacks. Therefore intrusion detection system for protecting communications in such network is indispensable. In this paper we review the present state of the art of the intrusion detection systems (IDS) and discover the research gaps that give insights into the potential research areas with respect to intrusion detection in MANET. Our focus is on host based IDS, network based IDS and agent based IDS. This paper also covers attacks specific to MANET such wormhole, sinkhole etc. The existing intrusion detection systems found in the literature operate on both protocols dependent and independent approaches. Energy efficiency, routing protocols, and various techniques used to safeguard MANETs from malicious attacks were explored. The research gaps found can help in choosing right paths for future work.***

Keywords: Secure communications in MANETs, intrusion detection system, routing protocols

1. Introduction

Mobile Ad Hoc Network (MANET) is a collection of nodes that form an on-demand network for communications with having fixed infrastructure. The nodes are mobile in nature with constrained resources. This has paved way for many vulnerabilities and security attacks in MANETs. Intrusion detection systems have been around for both wired and wireless networks. Kozushko (2003) [1] differentiated the network intrusion detection system from host based intrusion detection system be contrasting two architectures. However there is another kind of IDS known as agent-based IDS. Host based intrusion detection systems monitor a system's state and detects any intrusions. It monitors all operations within a computer and reports any operation that is not in tune with security policies of the system. The network based intrusion detection systems monitor the whole network and its traffic for discover unauthorized access to the network. An agent – based intrusion detection system is the system that contains multiple autonomous agents who involve in detecting malicious behavior in the network. In other words all agents cooperate with each other in order to detect intrusive activities.

There is plethora of literature on the three types of intrusion detection systems mentioned above. The host-based IDS is explored with different mechanism in many research articles including [1]-[19]. The techniques like genetic algorithms, bio-inspired technologies, MapReduce programming, reputation and liars concept, game-theory, and collaborative techniques are used. With respect to network – based intrusion detection systems, literature can be found in [21], [23], [24] and [25]. The techniques used include pattern matching, adaptive sub-eigenspace modeling, and friend-assisted mechanism.

Our contributions in this paper include the study of various techniques used for intrusion detection in MANETs and finding research gaps that provide insights required for future research. The remainder of this paper is structured as follows. Section 2 reviews and summarizes host based IDS. Section 3 provides review of network based IDS and its summary. Section 4 reviews attacks in MANETs. Section 5 throws light into energy efficient IDS and other models. Section 6 reviews and summarizes agent based IDS. Section 7 presents research gaps found in the survey while section 8 concludes the paper.

2. Host Based IDS

Tao Song (2007) [2] Proposed System Health and Intrusion Monitoring (SHIM) and Dynamic Registration and Configuration Protocol (DRCP) for achieving host-based intrusion detection system. Marchang and Datta (2008) [3] proposed an IDS which makes use of collaborative techniques. Basically it uses two techniques. The first one comes into picture between two nodes which are in the same radio range while the second one comes into picture when nodes do not locate in the same radio range. This solution is independent of routing protocols. Message passing and monitor node concept was used to achieve this. Otrok *et al.* (2008) [4] proposed an IDS that is based on game-theory. It can handle selfish nodes well and improves lifetime of MANET by balancing resource consumption and making nodes to participate in leader election truthfully. Bayesian Nash Equilibrium is used for optimal detection technique.

Mindinger and Boudec (2008) [5] used liars concept for analyzing reputation systems used in intrusion detection of MANETs. They brought about guidelines for effective reputation systems. Lauf *et al.* (2010) proposed embeddable and distributed IDS with local and global analysis for

detecting malicious nodes. The scheme was named as HybrIDS. Cheng and Tseng (2011) [6] presented a context adaptive IDS which ensures intelligent tradeoff between network lifetime and security. Grammatical programming and other evolutionary approaches are used by Sen and Clark (2011) [7] for IDS. Xenakis *et al.* (2011) [8] made a good review on comparison and evaluation of IDS. Zhang and Yeo (2011) [9] proposed an IDS known as distributed court system which was proved to be effective in environments like high mobile and hostility. Cho and Chen (2011) [10] proposed an adaptive IDS based on hierarchical group key management. Pakzad *et al.* (2011) [11] attempted to provide steps to improve IDS in MANET. Kumar *et al.* (2011) [11] also used GA for IDS implementation. Holtz built distributed IDS for MapReduce framework. Pastrana (2012) [12] explored classification algorithms used for IDS. Nikhil *et al.* (2012) [14] applied GA for intrusion detection. Bio – inspired methodology was used by Ramana *et al.* (2012) [15] for securing communication in MANET. Gargi *et al.* (2012) [14] explored neural networks for optimizing performance of DSR. Raghavendran *et al.* (2012) [15] used swarm intelligence for intelligent routing. An adaptive and highly scalable IDS named Kargus was proposed by Jamshed *et al.* (2012) [16]. Mohammad and Nagib (2012) [49] GA for secure and optimal routing. Random Waypoint Mobility Model was introduced by Abdulla (2012) [18] optimization of routing in MANET while Maan *et al.* (2012) [19] explored the role of artificial intelligence. Similar approach was explored in [58].

2.1 Summary of Host Based Intrusion Detection Systems

Author (s)	Year	Algorithm/Technique	Protocol	Study	Remarks
Tao Song [2]	2007	System Health and Intrusion Monitoring	Dynamic Registration and Configuration Protocol	Simulation and empirical.	
Razak *et al.* [20]	2008	ADCLI and ADCLU algorithms	Routing protocol independent solution	Simulation	Collaborative techniques are used in IDS
Otrok *et al.* [4]	2008	Game-theoretic IDS	Routing protocols	Simulation	Energy efficient leader election

3. Network Based IDS

Dharmapurikar *et al.* (2006) [21] proposed a novel algorithm known as pattern matching algorithm for packet inspection over network. It is a hardware implementable solution that is implemented using Bloom filters constructed using FPGA/VLSI chips. Shyu *et al.* (2007) [25] proposed Adaptive Sub-Eigenspace Modeling for network intrusion detection. Host layer and classification layer are used to identify attacks or intrusions. Moreover the approach followed here is "multi-agent design methodology" for intrusion detection. Razak *et al.* (2008) [3] proposed a novel detection mechanism known as friend-assisted IDS. This system combines host-based IDS with a network based IDS so as to have a global IDS operating in two tiers. Friend assisted approach is used in order to overcome the problem of maintaining a special server or component for authentication. The attacks are detected in the initial stages so as to avoid damage to MANET. The friend concept is used along with trust management and response time tied so as to improve the genuine behavior of nodes in MANET. The system heavily depends on relationships and expected to be a practical solution. Trust prediction and trust management approaches are used to have secure communications in [54]. Babu *et al.* (2013) [23] proposed a network-based IDS for MANET security. Kulkarni and Bakal (2014) [24] focused on network IDS that works on ensemble multi-classifiers in order to detect intrusions.

3.1 Summary of Network Based Intrusion Detection Systems

Author (s)	Year	Algorithm/Technique	Protocol	Study	Remarks
Dharmapurikar *et al.* [21]	2006	Pattern matching algorithm for network intrusion detection and Bloom filters.	TCP	Theoretical analysis and simulation	Bloom filters constructed using **FPGA/VLSI chips**
Shyu *et al.* [22]	2007	Adaptive Sub-Eigenspace Modeling	SNMP, CISCO	Simulation	Multi-agent design methodology

4. Attacks in Mobile Adhoc Networks

Sinkhole or Blackhole Attack was studied by Tseng and Culpepper (2005) [26]. Sinkhole attack is an attempt makes all traffic leading to malicious node which broadcasts shortest path routing which is actually fake. They proposed two sinkhole intrusion detection indicators which are based on the routing dynamics of DSR. Wormhole attack another attack carried out by adversaries in MANET. Such attack is caused when an attacker tunnels packets at a point in network and then uses them for replay towards other nodes in the network. Qian *et al.* (2007) [27] studied wormhole attacks in MANETs. They proposed a multi-path routing protocol named SAM which can effectively localize malicious nodes besides detecting wormhole attacks. It is useful for applications that prefer disjoint routes. Joseph *et al.* (2008) [28] focused on routing attacks in MANET. Especially their research was on the design issues of intrusion detection in MANETs. The techniques explored to know limitations include Logical rule-based techniques, classification techniques and probabilistic estimation based techniques. The solution suggested is optimized link state routing.

Kim *et al.* (2010) [29] presented a solution to handle sinkhole attacks in MANET by using a cooperative detection method. Su (2011) [30] explored selective blackhole attacks. They proposed anti blackhole mechanism to combat with blackhole attacks. Karloson *et al.* (2012) [31] explored routing security for preventing attacks. Chauhan *et al.* (2012) [32] explored key management for secure communications.

4.1 Attack Summary in MANETs

Author (s)	Year	Routing Protocol/ Attack	Solution	Study	Remarks
Tseng and Culpepper [26]	2005	DSR	Indicators of sinkhole intrusion proposed.	Simulation	
Qian *et al.* [27]	2007	Wormhole attack on multi-path routing.	New routing protocol named SAM	Statistical analysis	Localization of malicious nodes and wormhole attacks.
Joseph *et al.* [28]	2008	Routing attacks	Optimized link state routing	Logical deduction and simulation	Logical rule-based techniques, classification techniques and probabilistic estimation based techniques.

5. Energy Efficient and Other IDS Models

Kim *et al.* (2006) [33] proposed an energy efficient intrusion detection system based on a lifetime-enhancing monitoring node selection scheme. Tseng [50] proposed an IDS with two intrusion detection models namely authentication model and message exchange model and simulated the solutions using **GlomoSim**. Komninos *et al.* (2007) [51] proposed a two phase detection mechanism that detects unauthorized and compromised nodes in MANET. The detection mechanism acts on the operations of network and link layers. The IDS has detection, prevention and reaction to be robust against attacks. Patwardhan *et al.* (2008) [35] proposed a threshold-based IDS with traffic in the presence of AODV and IPv6. It has security features implemented using Certificate Authority (CA). Investigation has been made to know the mobility effect on performance of IDS. From this study they understood that collaborative IDS work in better way with less mobility and densely populated network. The effectiveness also depends on the bulk of data to be handled. Cabrera (2008) [36] proposed a distributed IDS that makes use of local anomaly index and ensemble methods for anomaly detection.

References

[1] Harley Kozushko. (2013). Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems. *Independent Study*. 11 (n.d), p-1-23
[2] H. Chris Tseng and B. Jack Culpepper. (2005). Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators.*Computers & Security*. 24 (n.d), 561-570.
[3] Hyunwoo Kim,Dongwoo Kim and Sehun Kim . (2006). Lifetime-enhancing selection of monitoring nodes for intrusion detection in mobile ad hoc networks. *aeu of electronics and communications*. 60 (n.d), p-248-250.
[4] CHIN-YANG HENRY TSENG. (2006). Distributed Intrusion Detection Models for Mobile Ad Hoc Networks. *Computer Science*. (n.d), p-1-144.
[5] Sarang Dharmapurikar, and John Lockwood. (2006). Fast and Scalable Pattern Matching for Network Intrusion Detection Systems. *IEEE*. 24 (n.d), p-1-1782-1792.
[6] Nikos Komninos Dimitris Vergados and Christos Douligeris. (2007). Detecting unauthorized and compromised nodes in mobile ad hoc networks. *science direct*. 5 (n.d), p-289-298.
[7] Lijun Qian, Ning Song and Xiangfang. (2007). Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach. *elsevier*. 30 (n.d), p-308-330.
[8] Tao Song. (2007). Formal Reasoning about Intrusion Detection Systems.*Computer Science*. . (n.d), p-1-206.
[9] MEI-LING SHYU, THIAGO QUIRINO, and ZONGXING XIE. (2007). Network Intrusion Detection through Adaptive Sub-Eigenspace Modeling in Multiagent Systems. *ACMTransactions on Autonomous and Adaptive Systems*. 2 (n.d), p-1-37.
[10] A. Patwardhan , J. Parker , M. Iorga , A. Joshi , T. Karygiannis and Y. Yesha. (2008). Threshold-based intrusion detection in ad hoc networks and secure AODV. *elsevier*. 6 (n.d), p-578–599.
[11] S.A. Razak , S.M. Furnell , N.L. Clarke and P.J. Brooke. (2008). Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks. *elsevier*. 6 (n.d), p-1151–1167.
[12] Ningrinla Marchang and Raja Datta. (2008). Collaborative techniques for intrusion detection in mobile ad-hoc networks. *elsevier*. 6 (n.d), p-508-523.
[13] Hadi Otrok , Noman Mohammed, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya. (2008). A game-theoretic intrusion detection model for mobile ad hoc networks. *elsevier*. 31 (n.d), p-708–721.
[14] Chandrasekar Ramachandran , Sudip Misra and Mohammad S. Obaidat. (2008). FORK: A novel two-

pronged strategy for an agent-based intrusion detection scheme in ad-hoc networks. *elsevier*. 31 (n.d), p-3855–3869.

[15] John Felix Charles Joseph , Amitabha Das , Boon-Chong Seet and Bu-Sung Lee . (2008). Opening the Pandora's Box: Exploring the fundamental limitations of designing intrusion detection for MANET routing attacks. *elsevier*. 31 (n.d), p-3178–3189.

[16] Joa B.D. Cabrera , Carlos Gutie´rrez, Raman K. Mehra. (2008). Ensemble methods for anomaly detection and distributed intrusion detection in Mobile Ad-Hoc Networks. *elsevier*. 9 (n.d), p-96–119.

[17] Jochen Mundinger and Jean-Yve Le Boud. (2008). Analysis of a reputation system for Mobile Ad-Hoc Networks with liars. *elsevier*. 65 (n.d), p-212–226.

[18] Emad Mohamed Fawwaz. (2008). Intrusion Detection for Mobile Ad hoc Networks. *Information Technology*. . (n.d), p-1-14.

[19] Nikos Komninos a,*, Christos Douligeris. (2009). LIDF: Layered intrusion detection framework for ad-hoc networks. *elsevier*. 7 (n.d), p-171-182

[20] R.Nallusamy, K.Jayarajan and Dr.K.Duraiswamy. (2009). Intrusion Detection In Mobile Ad Hoc Networks Using GA Based Feature Selection.*Computer Science and Telecommunications*. 5 (n.d), p-1-8.

[21] Ram Kumar Singh and T. Ramanujam. (2009). Intrusion Detection System Using Advanced Honeypots. *Computer Science and Information Security*. 2 (n.d), p-1-9

[22] Umunna Christian and Chezz Chetachi. (2009). Security and Performance Analysis of Topology-Based Intrusion Detection System in Ad Hoc Networks. *Master of Science in Electrical Engineering*. (n.d), p-1-60.

[23] S. Prasad, Y.P.Singh and C.S.Rai. (2009). Swarm Based Intelligent Routing for MANETs. *Recent Trends in Engineering*. 1 (n.d), p-1-6.

[24] Adrian P. Lauf , Richard . Peters, William H. Robinson. (2010). A distributed intrusion detection system for resource-constrained devices in ad-hoc networks. *elsevier*. 8 (n.d), p-253-266.

[25] Gisung Kim, YounggooHan and SehunKim. (2010). A cooperative-sinkholedetectionmethodformobileadhocnetworks. *elsevier*. 64 (n.d), p-390–397.

[26] Stefan K. Stafrace and Nick Antonopoulos. (2010). Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks.*elsevier*. 33 (n.d), p-619–638.

[27] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han. (2010). A Novel Cross Layer Intrusion Detection System in MANET.*IEEE*. (n.d), p-1-8.

[28] Saira Beg, Umair Naru, Mahmood Ashraf and Sajjad Mohsin. (2010). Feasibility of Intrusion Detection System with High Performance Computing: A Survey. *Computer Science and* . 1 (n.d), p-1-10.

[29] Shervin Ehrampoosh and Ali Khayatzadeh Mahani. (2010). Secure Routing Protocols: Affections on MANETs Performance. *comunication engineering* (n.d), p-1-6.

[30] Ming-Yang Su. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *elsevier*. 34 (n.d), p-107-117.

[31] Bo-Chao Cheng and Ryh-Yuh Tseng . (2011). A Context Adaptive Intrusion Detection System for MANET. *elsevier*. 34 (n.d), p-310–318

[32] Sevil Sen and John A. Clark. (2011). Evolutionary computation techniques for intrusion detection in mobile ad hoc networks. *elsevier*. 55 (n.d), p-3441–3457

[33] Christos Xenakis ,Christoforos Panos and Ioannis Stavrakakis . (2013). A comparative evaluation of intrusion detection architectures for mobile ad hoc networks. *elsevier*. 30 (n.d), p-63-80

[34] Da Zhang and Chai Kiat Yeo. (2011). Distributed Court System for intrusion detection in mobile ad hoc networks. *elsevier*. 30 (n.d), p-5 5 5 -5 7 0.

[35] Jin-Hee Cho and Ing-Ray Chen. (2011). Performance analysis of hierarchical group key management integrated with adaptive intrusion detection in mobile ad hoc networks. *elsevier*. 68 (n.d), p-58-75.

[36] farzaneh pakzad,marjan kuchaki rafsanjani and arsham borumand saeid. (2011). the improvement steps of intrusion detection system arrchitecture of manets. *mathematics & statistics*. 22 (n.d), p-1-13.

[37] Jin-Hee Cho,AnanthramSwami andIng-RayChen. (2012). Modeling andanalysis of trust management with trust chain optimization in mobile adhoc networks. *Elsevier*. 35 (n.d), p-1001–1012.

[38] Sergio Pastrana,Aikaterini Mitrokosa,Agustin Orfila andPedro Peris-Lopez. (2012). Evaluation of classification algorithms for intrusion detection in MANETs. *Elsevier*. 36 (n.d), p-217–225.

[39] Kumar Nikhil,Swati Agarwal and Pankaj Sharma. (2012). APPLICATION OF GENETIC ALGORITHM IN DESIGNING A SECURITY MODEL FOR MOBILE ADHOC NETWORK. (n.d), p-1-7.

[40] V. Venkata Ramana,Dr. A. Ramamohan Reddy andDr. K. Chandra sekaram. (July 2012). Bio Inspired Approach to Secure Routing in MANETs. *Artificial Intelligence & Applications*. 3 (n.d), p-1-10.

[41] Rajesh Gargi, Yogesh Chaba and R.B.Patel. (2012). Improving the Performance of Dynamic Source Routing Protocol by Optimization of Neural Networks. *Computer Science Issues*. 9 (n.d), p-1-9

[42] CH. V. Raghavendran,G. Naga Satish and P. Suresh Varma . (2012). Intelligent Routing Techniques for Mobile Ad hoc Networks using Swarm Intelligence. *Intelligent Systems and Applications*. 1 (n.d), p-81-89

[43] Anjum A. Mohammed. (2012). Optimal Routing In Ad-Hoc Network Using Genetic Algorithm. *Advanced Networking and Applications*. 3 (n.d), p-1323-1328.

[44] Jiwa Abdullah. (2012). Performance of QOSRGA Routing Protocol for MANET with Random Waypoint Mobility Model. *Advanced Science and Technology*. 40 (n.d), p-1-16

[45] Neeti Maan and Dr. Ravindra Kumar Purwar. (2012). Role of Artificial intelligence in MANET. *Advanced Research in Computer Engineering & Technology*. 1 (n.d), p-2278 – 1323

[46] Jonny Karlsson ,Laurence S. Dooley and Göran Pulkkis. (2012). Routing Security in Mobile Ad-hocNetworks. *Informing Science and Information Technology*. 9 (n.d), p-1-15.

[47] Kamal Kumar Chauhan and Amit Kumar Singh Sanger. (2012). Securing Mobile Ad hoc Networks: Key Management and Routing. *AdHoc Networking Systems*. 2 (n.d), p-1-11.
[48] Hui Xia , Zhiping Jia , Xin , Lei Ju , Edwin H.-M. Sha. (2013). Trust prediction and trust-based source routing in mobile ad hoc networks.*elsevier*. 11 (n.d), p-2096-2114.
[49] ShahaboddinShamshirband , NorBadrulAnuar , MissLaihaMatKiah and AhmedPatel. (2013). An appraisalanddesignofamulti-agentsystembasedcooperative wirelessintrusiondetectioncomputationalintelligencetechnique. *elsevier*. 26 (n.d), p-2105-2127
[50] Wei Wang , Huiran Wanga, Beizhan Wang, Yaping Wang and Jiajun Wang. (2013). Energy-aware and self-adaptive anomaly detection scheme based on network tomography in mobile ad hoc networks.*elsevier*. 220 (n.d), p-580-602.
[51] Vijaya Bhaskar and Ch , Dr. D.S. R. Murthy. (2013). A Reliable Routing Approach in Mobile AdHoc Network based on Genetic Algorithms.*elsevier*. 2 (n.d), p-1-5.
[52] Arun Kumar. R, Abhishek M. K, Tejashwini. Niranjan J and T, Pradeep R.P. (2013). A Review on Intrusion Detection Systems in MANET.*Science and Innovative Technology*. 2 (.), p-2319-5967.
[53] Khalid Hussain, Abdul Hanan Abdullah, Khalid M. Awan and Zohair Ihsan. (2013). An Artificial Intelligence Based X-AODV Routing Protocol for MANET. *World Applied Sciences Journal*. 23 (.), p-541-548.
[54] Elhadi M. Shakshuki ,Nan Kang, and Tarek R. Sheltami. (2013). EAACK—A Secure Intrusion-Detection System for MANETs. *IEEE*. 60 (.), p-1-10
[55] Pankaj Vidhate, Yogita Wankhade. (2013). ROUTE OPTIMIZATION IN MANETS WITH ACO AND GA. *ijret*. 2 (.), p-587-590.
[56] CHILAKALAPUDI MEHER BABU, DR. UJWAL A. LANJEWAR, and CHINTA NAGA MANISHA. (2013). NETWORK INTRUSION DETECTION SYSTEM ON WIRE LESS MOBILE ADHOC NETWORKS. *ijarcce*. 2 (.), p-1495-1500.
[57] Vishal Gupta. (2013). Route Optimization in MANET using FIGA. *ijeer*. 1 (.), p-38-45.
[58] Pankaj Vidhate, Yogita Wankhade. (2013). ROUTE OPTIMIZATION IN MANETS WITH ACO AND GA. *ijret*. 2 (.), p-587-590.
[59] Ehsan Amiri, Hassan Keshavarz, Hossein Heidari, Esmaeil Mohamadi and Hossein Moradzadehe. (2014). Intrusion Detection Systems in MANET: A Review. *elsevier*. . (.), p-453-459
[60] Ing-Ray Chen , Jia Guo , Fenye Bao , Jin-Hee Cho. (2014). Trust management in mobile ad hoc networks for bias minimization and application performance maximization. *e*. . (.), p-59-74
[61] Amin Hassanzadeh, Ala Altaweel, Radu Stoleru. (2014). Traffic-and-resource-aware intrusion detection in wireless mesh networks. *elsevier*. 21 (.), p-18-41.
[62] Abdulsalam Basaba, Tarek Sheltamia and Elhadi Shakshuki. (2014). Implementation of A3ACKs intrusion detection system under various mobility speeds. *elsevier*. 32 (.), p-571-578
[63] Lalit Kulkarni and Jagdish Bakal. (2014). Intrusion Detection System (IDS) for Wireless Ad-hoc Networks using Evolution Identification on Streaming Network Data for Detecting Unknown Network Attacks. *ijrcct*. 3 (.), p-213-218.
[64] Binod Kumar Pattanayak and Mamata Rath. (2014). A MOBILE AGENT BASED INTRUSION DETECTION SYSTEM ARCHITECTURE FOR MOBILE AD HOC NETWORKS. *Journal of Computer Science*. 10 (.), p-970-975.

Appendix

Acronyms

DSR	Dynamic Source Routing
MANET	Mobile Ad Hoc Networks
SIIS	Sinkhole Intrusion Indicators
IDS	Intrusion Detection System
DIDS	Distributed Intrusion Detection System
SAM	Statistical analysis of multi-path.
CA	Certificate Authority