Privacy Preserving Error Control Data Detection of Packet Reducing In Wireless Adhoc Networks

Dr.V.Goutham[1], K.Rajyalaxmi[2], P.Shiva parvathi [3]
[1,2,3]Department of Computer Science and Engineering, Teegala Krishna Reddy Engineering College, Meerpet, Telangana, India

Abstract— In this Privacy preserving and Error Control Data Detection of packet reducing in wireless adhoc networks, while noticing a sequence of packet losses in the network, it determines whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop. Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network. Malicious nodes that are part of the route deed their information of the communication framework to selectively drop a small amount of packets precarious to the network concert. The packet dropping rate is analogous to the channel error rate, conventional algorithms that are centred on perceiving the packet loss rate cannot accomplishing satisfactory detection truthfulness. To recover the detection accuracy, and exploiting the correlations between lost packets, to ensure truthful calculation of these correlations, a homomorphic linear authenticator (HLA) based public auditing architecture is introduced that allows the detector to verify the truthfulness of the packet loss information reported by nodes.

Index Terms—Packet dropping, secure routing, attack detection, homomorphic linear signature, auditing

1 INTRODUCTION

In a multi-hop wireless network, nodes collaborate in relaying/ routing traffic. An adversary can abuse this obliging nature to launch attacks. Once comprised in a route, the adversary twitches dropping packets. In the most Spartan form, the malicious node merely stops accelerating every packet received from upstream nodes, completely unruly the path between the source and the destination. Ultimately, such a severe denial-of-service (DoS) attack can paralyze the network by partitioning its topology. Even though persistent packet dropping can effectively degrade the performance of the network, from the attacker's standpoint such an "always-on" attack has its disadvantages. First, the unceasing presence of extremely high packet loss rate at the malicious nodes makes this type of attack easy to be detected [25]. Second, once being detected, these attacks are easy to mitigate. For example, in case the attack is detected but the malicious nodes are not identified, one can use the randomized multi-path routing algorithms [28], [29] to bypass the black holes engendered by the attack, probabilistically eradicating the attacker's threat. If the malicious nodes are also identified, their threats can be completely disregarded by simply deleting these nodes from the network's routing table. A malicious node that is part of the route can exploit its knowledge of the network protocol and the communication context to launch an insider attack—an attack that is recurrent, but can achieve the same performance degradation effect as a persistent attack at a much lower risk of being detected. Precisely, the malicious node may evaluate the importance of various packets, and then drop the small amount that are deemed highly critical to the operation of the network. For example, in a frequency-hopping network, these could be the packets that convey frequency hopping sequences for network-wide frequency-hopping synchronization; in an ad hoc perceptive radio network, they could be the packets that carry the idle channel lists (i.e., white spaces) that are used to inaugurate a network-wide control channel. By steering these highly critical packets, the authors in [21], [24], [25] have shown that an alternating insider attacker can cause significant damage to the network with low probability of being caught. In this Privacy preserving and Error Control Data Detection of packet reducing in wireless adhoc networks, we are interested in opposing such an insider attack. In particular, we are interested in the problem of sensing the manifestation of selective packet drops and identifying the malicious node(s) responsible for these drops. Spotting selective packet-dropping attacks is tremendously challenging in a highly dynamic wireless environment. The exertion comes from the requirement that we need to not only detect the place (or hop) where the packet is dropped, but also identify whether the drop is intentional or Unintentional. Explicitly, due to the open nature of wireless Medium, a packet drop in the network could be caused by harsh channel conditions . So, the insider attacker can facade under the background of harsh channel conditions. In this case, just by observing the packet loss rate is not enough to accurately identify the exact cause of a packet loss. The above problem has not been well addressed in the literature. In this Privacy preserving and Error Control Data Detection of packet reducing in wireless adhoc networks, an exact algorithm for detecting selective packet drops made by insider attackers is developed. Thisalgorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of thepacket-loss bitmap—a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions. The basic idea behind this method is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the stochastic Progressions that portray the two phenomena exhibit different correlation structures.This algorithm takes into account the cross-statistics between lost packets to make a more informative decision, and thus is in sharp contrast to the conventional methods that rely only on the distribution of the number of lost packets. The main experiment in this mechanism lies in how to assure that the packet-loss bitmaps reported by individual nodes along the route are truthful, i.e., reflect the actual status of each packet transmission. Such reliability is essential for correct calculation of the correlation between lost packets. This challenge is not trivial, because it is natural for an attacker to report false information to the detection algorithm to avoid being detected[8]. For example, the malicious node may understate its packet-loss bitmap, i.e., some packets may have been dropped by the node but the node reports that these packets have been accelerated. Therefore, some auditing mechanism is needed to verify the truthfulness of the reported information. Considering that a typical wireless device is resource-constrained, we also require that a user should be able to delegate the burden of auditing and detection to some public server to save its own resources. This solution to the above public-auditing problem is fabricated based on the homomorphic linear authenticator (HLA) cryptographic primitive [2], [3], [7], which is basically a signature scheme widely used in cloud computing and storage server systems to provide a proof of storage from the server to entrusting clients [3]. However, direct application of HLA does not solve thisproblem well, mainly because in thisproblem setup, there can be more than one malicious node along the route. These nodes may collude (by exchanging information) during the attack and when being asked to submit their reports[9]. For example, a packet and its associated HLA signature may be dropped at an upstream malicious node, so a downstream malicious node does not receive this packet and the HLA signature from the route. However, this downstream attacker can still open a back-channel to request this information from the upstream malicious node. When being audited, the downstream malicious node can still provide valid proof for the reception of the packet. So packet dropping at the upstream malicious node is not detected. Such collusion is unique to this problem, because in the cloud computing/storage server scenario, a file is uniquely stored at a single server, so there are no other parties for the server to collude with. We show that this new HLA construction is collusion-proof. This construction also provides the following new features. First, privacy-preserving: the public auditor should not be able to decern the content of a packet delivered on the route through the auditing information submitted by individual hops, no matter how many independent reports of the auditing information are submitted to the auditor. Second, this construction incurs low communication and storage overheads at intermediate nodes. This makes this mechanism applicable to a wide range of wireless devices, including low-cost wireless sensors that have very limited bandwidth and memory capacities. This is also in sharp contrast to the typical storage-server scenario, where bandwidth/storage is not considered an issue. Last, to significantly reduce the computation overhead of the baseline constructions so that they can be used in computation-constrained mobile devices, a packet-block-based algorithm is proposed to achieves scalable signature generation and detection [6]. This mechanism allows one to trade detection accuracy for lower computation complexity.

2 BACKGROUND

Depending on how much weight a detection algorithm gives to link errors relative to malicious packet drops, the related work can be classified into the following two categories. The first category aims at high malicious dropping rates, where most (or all) lost packets are caused by malicious dropping. In this case, the impact of link errors is ignored. Most related work falls into this category. Based on the methodology used to identify the attacking nodes, these works can be further classified into these sub-categories. The first sub-category is based on credit systems [9], [4], [10]. A credit system provides an incentive for cooperation. A node receives credit by relaying packets for others, and uses its credit to send its own packets. As a result, a maliciously node that continuous to drop packets will eventually deplete its credit, and will not be able to send its own traffic. The second sub-category is based on reputation systems [19], [20]. A standing system depends on neighbors to monitor and identify misbehaving nodes. A node with a high packet dropping rate is given a bad reputation by its neighbors. This reputation information is propagated periodically throughout the network and is used as an important metric in selecting routes[5]. Subsequently, a malicious node will be excluded from any route. The third sub-category of works relies on end-to-end or hop-to-hop acknowledgements to directly locate the hops where packets are lost [18]. A hop of high packet loss rate will be excluded from the route. The fourth subcategory addresses the problem using cryptographic methods. For example, the work in [17] utilizes Bloom filters to construct proofs for the forwarding of packets at each node. By examining the relayed packets at successive hops along a route, one can identify suspicious hops that exhibit high packet loss rates. Similarly, the method in [16] traces the forwarding records of a particular packet at each intermediate node by formulating the tracing problem as a Renyi-Ulam game. The first hop where the packet is no longer forwarded is considered a suspect for misbehaving. The second category targets the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible. Certain knowledge of the wireless channel is necessary in this case. The authors in [2] proposed to shape the traffic at the MAC layer of the source node according to a certain statistical distribution, so that intermediate nodes are able to estimate the rate of received traffic by sampling the packet arrival times. By comparing the source traffic rate with the estimated received rate, the detection algorithm decides whether the discrepancy in rates, if any, is within a reasonable range such that the difference can be considered as being caused by normal channel impairments only, or caused by malicious dropping, otherwise. The works in [13] and [1] proposed to detect malicious packet dropping by counting the number of lost packets. If the number of lost packets is significantly larger than the expected packet loss rate made by link errors, then with high probability a malicious node is contributing to packet losses [4]. All methods mentioned above do not perform well when malicious packet dropping is highly selective. More specifically, for the credit-system-based method, a malicious node may still receive enough credits by forwarding most of the packets it receives from upstream nodes. Similarly, in the reputation-based approach, the malicious node can maintain a reasonably good reputation by forwarding most of the packets to the next hop. While the Bloom-filter scheme is able to provide a packet forwarding proof, the correctness of the proof is probabilistic and it may contain errors. For highly selectively attacks (low packet-dropping rate), the intrinsic error rate of Bloom filer significantly undermines its detection accuracy. As for the acknowledgement-based method and all the mechanisms in the second category, merely counting the number of lost packets does not give a sufficient ground to detect the real culprit that is causing packet losses. This is because the difference in the number [3] of lost packets between the link-error-only case and the link-error-plus-malicious-dropping case is small when the attacker drops only a few packets. Consequently, the detection accuracy of these algorithms deteriorates when malicious drops become highly selective. This study targets the challenging situation where link errors and malicious dropping lead to comparable packet Loss rates. The effort in the literature on this problem has been quite [1] preliminary, and there is a few related works. Note that the cryptographic methods proposed in [4] to counter selective packet jamming target a different issue than the detection problem studied in this Privacy preserving and Error Control Data Detection of packet reducing in wireless adhoc networks. The methods in [20] delay a jammer from recognizing the significance of a packet after the packet has been successfully transmitted, so that there is no time for the jammer to conduct jamming based on the content/importance of the packet. Instead of trying to detect any malicious behavior, the approach in [20] is proactive, and hence incurs overheads regardless of the presence or absence of attackers.

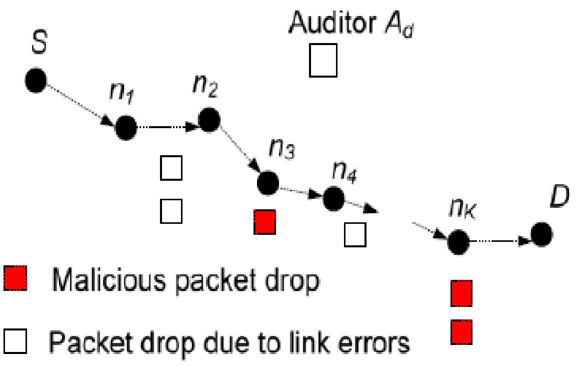

Fig. 1. Network and attack model.

3 RELATED WORK

3.1 Network and Channel Models

we mainly focus on static or quasi-static wireless ad hoc networks,that the network topology and link characteristics remain unchanged for a relatively long period of time. Example networks include wireless mesh networks (WMNs) and ad hoc networks designed in nomadic computing. Addition to a highly mobile environment is out of this scope and will be considered in the future work. The wireless channel of each hop along PSD as a random process that alternates between good and bad states. Packets conveyed during the good state are successful, and packets conducted during the bad state are lost. In divergence to the classical Gilbert-Ellioit (GE) channel Model, here we do not assume any Markovian property on the channel behavior. We only require that the sequence of sojourn times for each state follows a stationary distribution, and the autocorrelation function of the channel state. Here we limit this study to quasi-static networks,[19] whereby the path PSD remains unchanged for a relatively long time, so that the link error statistics of the wireless channel is a wide-sense stationary (WSS) random process. Detecting malicious packet drops may not be a concern for highly mobile networks, because the fast-changing topology of such networks makes route disruption the dominant cause for packet losses. In this case, continuing stable connectivity between nodes is a greater concern than identifying malicious nodes.

3.2 Adversarial Model

The goal of the adversary is to degrade the network's performance by maliciously dropping packets while remaining undetected. We assume that the malicious node has knowledge of the wireless channel, and is aware of the algorithm used for misbehavior detection [20]. It has the freedom to choose what packets to drop.Under the system and adversary models defined above, we address the problem of recognising the nodes on PSD that drop packets maliciously. We require the detection to be completed by a public auditor that does not have knowledge of the secrets held by the nodes on PSD. When a malicious node is identified, the auditor should be able to construct a publicly demonstrable proof of the misbehavior of that node. The construction of such a proof should be privacy preserving, i.e., it does not reveal the original information that is transmitted on PSD. In addition, the detection mechanism should incur low communication and storage overheads, so that it can be applied to a wide variety of wireless networks.

IV. PROPOSED SYSTEM: CORRELATION DETECTION SCHEME

The proposed mechanism is based on perceiving the correlations between the lost packets over each hop of the path. The basic idea is to model the packet loss process of a hop as a random process blinking between 0 (loss) and 1 (no loss). Specifically, consider that a sequence of M packets that are transmitted sequentially over a wireless channel. By noting whether the transmissions are successful or not, the receiver of the hop obtains a bitmap[17] .The correlation of the lost packet is calculated as the auto-correlation function of this bitmap. Under different packet dropping conditions, i.e., link-error versus malicious dropping, the instantiations of the packet-loss random process should present distinct dropping patterns (represented by the correlation of the instance). This is true even when the packet loss rate is similar in each instantiation. It is simulated the auto-correlation functionsm of two packet loss processes, one caused by 10 percent link errors, and the other by 10 percent link errors plus 10 percent malicious uniformly-random packet dropping.

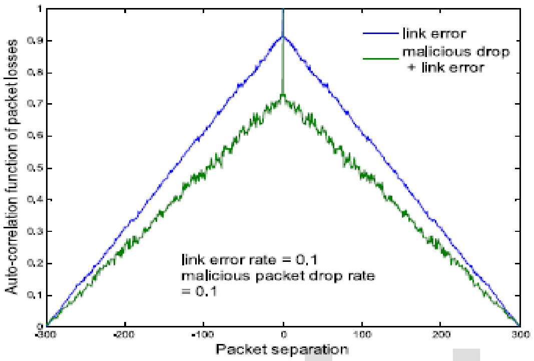

Fig. 2. Comparison of correlation of lost packets

The value of exploiting the correlation of lost packets can be better illustrated by inspecting the inadequacy of the conventional method that relies only on the distribution of the number of lost packets[16]. To decorously calculate the correlation between lost packets, it is critical to enforce a truthful packet-loss bitmap report by each node. We use HLA cryptographic primitive for this purpose. The basic idea of this method is as follows. An HLA scheme allows the source, which has knowledge of the HLA secret key, to generate HLA signatures, M independent messages respectively. The source sends out the along the route. The HLA signatures are made in such a way that they can be used as the basis to construct a valid HLA signature for any arbitrary linear combination of the messages, can be constructed by a node that does not have knowledge of the secret HLA key if and only if the node has full knowledge So, if a node with no knowledge of the HLA[15] secret key provides a valid signature , it implies that this node must have received all the signatures.

4.1 Computation Capability

Computation Requirements:

Most of the computation is done at the source and at the public auditor. We consider the public auditor as a dedicated service provider that is not embarrassed by its computing capacity. So the computational overhead should not be a factor limiting the application of the algorithm at the public auditor. On the other hand, the proposed algorithm requires the source node to generate K HLA signatures for a K-hop path for each data packet. The generation of HLA signatures is computationally expensive, and may limit the applicability of the algorithm.

REDUCING COMPUTATION OVERHEAD: BLOCK-BASED HLA SIGNATURE GENERATION AND DETECTION

A block-based solution that can reduce this overhead by multiple folds. The main idea is to make the HLA signature scalable: instead of generating per-packet HLA signatures, per-block HLA signatures will be generated, where a block consists of L > 1 packets. Accordingly, the detection will be extended to blocks, and each bit in the packet-loss bitmap represents a block of packets rather than a single packet. The details of this extension are elaborated as follows[14]. In the Packet Transmission Phase, rather than generating HLA signatures for every packet, now the signatures are based on a block of packets. In particular, L consecutive packets are deemed as one block. Accordingly, the stream of packets is now considered as stream of blocks. The block based HLA signature and detection mechanism can in general reduce the computation overhead by L folds[13]. However, the coarser representation of lost packets makes it difficult to accurately capture the correlation between them. Therefore, it is expected that the reduced computational overhead comes at the cost of less detection accuracy.

V. PERFORMANCE EVALUATION

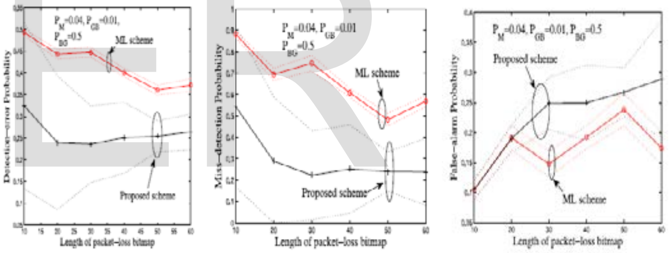

Fig: overall detection-error probability Fig: Miss-detection probability Fig: False-alarm probability

In each subfigure above, there are two sets of curves, representing the proposed algorithm and the optimal ML scheme, respectively. In each set of curves, the one in the middle represents the mean, and the other two represent the 95 percent confidence interval. In general, the detection accuracy of both algorithms improves. This is not startling, because malicious packet drops become more statistically discernible as the attacker starts to drop more packets. The proposed algorithm provides slightly higher false-alarmrate but pointedly lower miss-detection probability (subfigure (b)) than the ML scheme [12]. A low miss-detection probability is very desirable in this context, because it means a malicious node can be detected with a complex probability. The slightly higher false-alarm rate should not be a problem, because a false alarm can be easily recognized and fixed in the post-detection investigation phase. Most importantly, the overall detection-error probability of the proposed scheme is lower than that of the ML scheme .Weare especially interested in the regime when PM is comparable to the average packet loss rate due to link errors[11]. This rule represents the consequence in which the attacker hides its drops in the background of link errors by mimicking the channel-related loss rate. In this case, the ML scheme cannot correctly differentiate between link errors and malicious drops. This proposed algorithm, on the other hand, achieves a much better detection accuracy, as a result, the total detection-error rate of the proposed algorithm is about 35 percent. When PM is increased to 0.04, Perror of the proposed scheme reduces to only 20 percent, which is roughly half of the error rate of the ML scheme at the same PM. Remembering that the detection error rate of the ML scheme is the lowest among all detection schemes that only utilize the distribution of the number of lost packets, the lower detection-error rate of the proposed scheme shows that exploiting the correlation between lost packets helps in identifying the real cause of packet drops more accurately. The effect of exploiting the correlation is especially visiblewhen the malicious packet-drop rate is comparable with the link error rate. Meanwhile, we also note that the 95 percent confidence interval of the proposed scheme is wider than that of theML scheme. This is because the decision variable in the proposed scheme is a second-order function of the random packet loss process, while the decision variable in the ML scheme (i.e., number of lost packets) is a first order function of the same packet loss process. As a result, the decision variable of the proposed scheme possesses more randomness than that of the ML scheme, as reflected by the wider 95 percent confidence interval. The two-state Markovian GE channel model has a short range dependence, i.e., the correlation between two points of the fluctuation process decays rapidly with the increase in the separation between these points. This short-range dependence is reflected in an exponentially decaying autocorrelation function for the channel. As a result, a good estimation of the autocorrelation function can be derived as long as M is long enough to cover the function's short tail. This phenomenon implies that a node does not need to maintain a large packet-reception Database in order to achieve a good detection accuracy under the proposed scheme[10]. It also explains the low storage overhead incurred by this scheme.

6. CONCLUSION

In this Privacy preserving and Error Control Data Detection of packet reducing in wireless adhoc networks, it is compared with conventional detection algorithms that utilize only the distribution of the number of lost packets, manipulating the correlation between lost packets significantly expands the accuracy in detecting malicious packet drops. Such improvement is especially visible when the number of maliciously dropped packets is comparable with those caused by link errors. To appropriately calculate the correlation between lost packets, it is perilous to acquire truthful packet-loss information at individual nodes. We established an HLA-based public auditing architecture that ensures truthful packet-loss reporting by individual nodes. This architecture is collusion proof, requires relatively high computational capacity at the source node, but incurs low communication and storage overheads over the route. In this Privacy preserving and Error Control Data Detection of packet reducing in wireless adhoc networks we have assumed that source and destination are truthful in following the established protocol because delivering packets end-to-end is in their interest. Misbehaving source and destination will be pursued in this future research. Moreover, in this Privacy preserving and Error Control Data Detection of packet reducing in wireless adhoc networks, as a proof of concept, we mainly focused on showing the feasibility of the anticipated cypto-primitives and how second order statistics of packet loss can be utilized to improve detection accuracy. As a first step in this direction, this exploration mainly accentuate the essential structures of the problem, such as the untruthfulness nature of the attackers, the public verifiability of proofs, the privacy-preserving requirement for the auditing process, and the randomness of wireless channels and packet losses.

REFERENCES

[1] J. N. Arauz, "802.11 Markov channel modeling," Ph.D. dissertation, School Inform. Sci., Univ. Pittsburgh, Pittsburgh, PA, USA, 2004.

[2] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007, pp. 598–610.

[3] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319–333.

[4] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

[5] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.

[6] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.

[7] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," J. Cryptol., vol. 17, no. 4, pp. 297–319, Sep. 2004.

[8] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf., 2002, pp. 226–236.

[9] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in selforganizing mobile ad hoc networks," ACM/Kluwer Mobile Netw. Appl., vol. 8, no. 5, pp. 579–592, Oct. 2003.

[10] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," presented at the First Workshop Modeling Optimization Mobile, Ad Hoc Wire less Netw., Sophia Antipolis, France, 2003.

[11] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "Routing amid colluding attackers," in Proc. IEEE Int. Conf. Netw. Protocols, 2007, pp. 184–193.

[12] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable secure routing for

ad hoc networks," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 –9.

[13] T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim, "Detecting malicious packet dropping in the presence of collisions and chan nel errors in wireless ad hoc networks," in Proc. IEEE Int. Conf. Commun., 2009, pp. 1062–1067.

[14] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation- based incentive scheme for ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2004, pp. 825–830.

[15] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," in Ad Hoc Networking. Reading, MA, USA: Addison-Wesley, 2001, ch. 5, pp. 139–172.

[16] W. Kozma Jr. and L. Lazos, "Dealing with liars: Misbehavior identification via Renyi-Ulam games," presented at the Int. ICST Conf. Security Privacy in Commun. Networks, Athens, Greece, 2009.

[17] W. Kozma Jr., and L. Lazos, "REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. ACM Conf. Wireless Netw. Secur., 2009, pp. 103–110.

[18] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowl edgement-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2006.

[19] Y. Liu and Y. R. Yang, "Reputation propagation and agreement in mobile ad-hoc networks," in Proc. IEEE WCNC Conf., 2003, pp. 1510–1515.

[20] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom Conf., 2000, pp. 255–265.

[21] G. Noubir and G. Lin, "Low-power DoS attacks in data wireles lans and countermeasures," ACM SIGMOBILE Mobile Comput. Commun. Rev., vol. 7, no. 3, pp. 29–30, Jul. 2003.

[22] V. N. Padmanabhan and D. R. Simon, "Secure traceroute to detect faulty or malicious routing," in Proc. ACM SIGCOMM Conf., 2003, pp. 77–82.

[23] P. Papadimitratos and Z. Haas, "Secure message transmission in mobile ad hoc networks," Ad Hoc Netw., vol. 1, no. 1, pp. 193–209, 2003.

AUTHORS

[1] Dr V. Goutham is a Professor and Head of the Department of Computer Science and Engineering at Tegala Krishna Reddy Engineering College affiliated to J.N.T.U Hyderabad. He received Ph.d from Acharya Nagarjuna University M.Tech from Andhra University. He worked for various MNC Companies in Software Testing and Quality as Senior Test Engineer. His research interests are Software Reliability Engineering, software testing, software Metrics, and cloud computing

[2] Ms. K.Rajyalaxmi is working as a Assistant Professor in the Department of Computer Science And Engineering at Tegala Krishna Reddy Engineering College affiliated to J.N.T.U Hyderabad.

[3] Mrs. P.Shiva parvthi Department of Computer Science and Engineering at Tegala Krishna Reddy Engineering College affiliated to J.N.T.U Hyderabad.