IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

Secure Routing and Truthfull Based Packet Drop Attacks in Wireless Ad Hoc Network

T. Parameshwaran[1], Dr. C. Palanisawmy[2], R. D. Saranyadevi[3]

Department of Computer Science and Engineering, Anna University, Regional Campus-Coimbatore[1,3]

Professor& Head, Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam[2]

Abstract: Packet dropping attack, which is a crucial issue in networks. Link error and malicious packet dropping are two sources for packet losses. While observing a sequence of packet losses in the network, it is difficult to identify whether the loss is due to link errors or malicious nodes. Packet may be dropped during forwarding of routing information or during data forwarding. Dropping can be due to presents of malicious nodes or due to link error. Hence to improve the detection accuracy, the correlations between lost packets is identified. The proposed method is based on detecting the bitmap between the lost packets over each hop of the path. It 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 Audit based elliptic curve cryptography (AECC) which describes the status of each packet in a sequence of packet transmission. Therefore, by detecting the correlations between the lost packets, one can decide whether the packet loss is purely due to link errors, or is a combined effect of malicious drop and link error. Audit node is used to identify the malicious node or not. The Audit management in the WSN is like usually RREQ and RREP message passing between nodes. The energy is used to distinguish between altruism and selfish node.

Keywords: Packet dropping, Secure routing, Attack detection, AECC, Auditing.

I. INTRODUCTION

Wireless ad hoc network provides rapid on-demand network deployment without the need for the establishment of infrastructure. Nodes spontaneously self-organize into a network by coordinating network functions in a collaborative manner. Because of their infrastructure-less and autonomous nature, ad hoc networks find application on many domains including disaster relief operations, vehicular networks, tactical communications, environmental monitoring, and others.

The number of different threats and attacks can be categorized into a number of different areas that they target. The first is to consider the level of the attack which can be perceptual where the human perception is targeted using the media as a bearer. It may be broadcasting false information or just observation of social behavior to be able to alter decision processes. Secondly the attacks can target the information itself where interception and eavesdropping comes naturally in thought. Of the more active nature of these attacks might be the creation of false messages injected into networks. Also the denial or degradation of network services is a form of active attack on the information level. In this category application level attacks such as Trojan horses or viruses and the like are also included. The physical attacks are the third category. The passive nature of this category can be radiation interception or inductive wiretapping. The more hands on attacks include theft of equipment, cryptographic or physical keys, and different storage medias.

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 intermittent, but can achieve the same performance degradation effect as a persistent attack at a much lower risk of being detected. Specifically, 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 cognitive radio network, they could be the packets that carry the idle channel lists (i.e., white spaces) that are used to establish a network-wide control channel.

By targeting these highly critical packets, the authors in have shown that an intermittent insider attacker can cause significant damage to the network with low probability of being caught. In this paper, we are interested in combating such an insider attack. In particular, we are interested in the problem of detecting the occurrence of selective packet drops and identifying the malicious node(s) responsible for these drops.

II. RELATED WORK

The 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. An method called reputation systems. A reputation system relies 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. Consequently, 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. A hop of high packet loss rate will be excluded from the route. In exiting system use cryptographic methods. For example, the work in 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. 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. 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 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.

In exiting methods 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 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.

III. PROBLEM STATEMENT

Detecting selective packet-dropping attacks is extremely challenging in a highly dynamic wireless environment. The difficulty 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. Specifically, due to the open nature of wireless medium, a packet drop in the network could be caused by harsh channel conditions (e.g., fading, noise, and interference, a.k.a., link errors), or by the insider attacker. In an open wireless environment, link errors are quite significant, and may not be significantly smaller than the packet dropping rate of the insider attacker. So, the insider attacker can camouflage 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.

IV. PROPOSED SYSTEM

The malicious node may identify the importance of various packets and then it drops few packets, which are important to the network operation. Since packet-dropping rate in this case is comparable to the channel error rate, existing detection algorithms cannot achieve satisfactory detection accuracy in identifying packet loss rate. Detection accuracy can be improved by exploiting the correlations between lost packets. The proposed method is based on detecting the public audit request algorithm between sources to destination the lost packets over each hop of the path. It 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 public audit request algorithm based Ad hoc On-Demand Distance Vector (AODV) (PARA-AODV) which describes the status of each packet in a sequence of packet transmission. Therefore, by detecting the correlations between the lost packets, one can decide whether the packet loss is purely due to link errors, or is a combined effect of malicious drop and link error.

A. Network Model

Multi-hop ad hoc network consisting of N nodes. Each node is responsible for relaying messages from source S to destination D. Here assume S is aware of nodes in path PSD, as in Ad hoc On-Demand Distance Vector (AODV). If AODV is used, the source can identify the nodes in PSD by performing a public audit request route operation. For simplicity, we number the nodes in PSD = {n1…… nk} in ascending order with k = {PSDj}. Node ni is upstream of nj if i < j and is downstream of nj if i > j. Also assume the source receives feedback from the destination when a significant performance drops in metrics of interest, such as throughput or delay occurs. Here assume that message integrity and authenticity can be verified using resource efficient cryptographic methods, i.e., nodes may use the Elliptic Curve Digital Signature Algorithm (ECDSA) that has been shown feasible for resource limited devices such as sensors. Finally, there are at least two independent paths to any destination, i.e., the network is two-connected. This assumption is essential for reaching every node in PSD through a disjoint path.

B. Adversarial Model

The adversarial assume the existence of multiple independently misbehaving nodes in PSD. Source or destination node in may be misbehaving, except the source and the destination which are assumed to be trusted. The

DOI 10.17148/IARJSET.2016.3607

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

goal of misbehaving nodes is to degrade throughput while remaining undetected. Misbehaving nodes are assumed to be aware of the mechanisms used for misbehaviour detection. collusion between malicious nodes: A covert communication channel may exist between any two malicious nodes, in addition to the path connecting them on PSD. As a result, malicious nodes can exchange any information without being detected by Ad or any other nodes in PSD. Malicious nodes can take advantage of this covert channel to hide their misbehavior and reduce the chance of being detected. For example, an upstream malicious node may drop a packet on PSD, but may secretly send this packet to a downstream malicious node via the covert channel. When being investigated, the downstream malicious node can provide a proof of the successful reception of the packet. This makes the auditor believe that the packet was successfully forwarded to the downstream nodes, and not know that the packet was actually dropped by an upstream attacker.

C. Public Audit Request and detection

The goal of the audit phase is to verify that the audited node ni forwards packets to the destination. When a node is audited, it has to provide proof of the packets it forwards. The proof is used by the source S to perform a simple membership test: Did node ni forward packets in set X to the next hop. The audit phase occurs in three steps: (a) sending an audit request, (b) constructing a behavioral proof, and (c) processing the behavioral proof. Once misbehavior has been detected in PSD, the source S selects a node ni to be audited based on the search phase. The source constructs a routing path PSni such that PSni and PSD are disjoint to avoid the audit request being dropped by the misbehaving node. The source also selects an audit packet count, acount, denoting the duration of the audit in terms of number of packets. The value of acount is user-definable and must be sufficiently large to differentiate misbehavior from normal packet loss rate. Lastly, S selects an initial packet sequence number astart, indicating the sequence number of the packet where the audit begins. The source signs the audit request to enable the verification of its authenticity and integrity.

When a node is audited, it constructs a behavioral proof of the set of all packets it forwards, from astart to astart + acount, denoted by X = {x1; x2…… xN}. Buffering packets themselves would require large amount of storage and significant overhead for transmission back to the source. On the other hand, request algorithm provide a compact representation of membership for a set X = {x1; x2……..xN} in an m-bit vector v with m ¿ N. For an empty set X, all m bits of v are initialized to zero. When S receives the behavioral proof from ni, it verifies its authenticity and discards vi if the signature check fails. If ni fails to respond to the audit request, S may re-transmit the request using alternative paths. After a certain number of reply failures, S assumes that the node ni is suspicious of misbehaving and continues with the algorithm execution. So far we have illustrated how the source S evaluates the behavior of node ni via auditing. We now show how S selects nodes for audit in order to identify misbehaving ones. We define the notion of a suspicious set V as the set of nodes ni 2 PSD which have not been shown honest.

Once the search process has converged on the misbehaving link, the two suspicious nodes ni; ni+1 are excluded in turn from the routing path to the destination D. The node preceding the first suspicious node will split the traffic between ni; ni+1 in turn. In Figure 5, S uses node n3 to exclude in turn suspicious nodes n4 and n5. The source alerts D that two suspicious nodes are monitored via path exclusion. The destination creates two request algorithm, vDi,vDi+1 corresponding to the packets routed through suspicious nodes ni; ni+1, and send them to S. The source compares vi; vi+1 with its own vSi ; vSi+1, and identifies the misbehaving node.

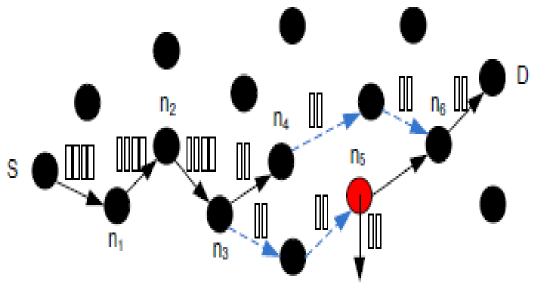

Fig.1 The AODV routing and pubic audit request

The proposed algorithm considers a sophisticated misbehaving node that changes its dropping pattern to avoid identification. Heret describe this behavior by an example. misbe having node n1 drops packets. The source uses binary search to identify the misbehavior, choosing node n3 to audit. The audit reply of n3 fails the membership test, reducing the suspicious set to V1 = fn1; : : : ; n3g. The source then audits node n2,. search is determine allowing n1 to predict the order that nodes are audited. Node n1 behaves honestly, thus n2's audit response passes the membership test. By changing its behavior, n1 removes himself from V.

Algorithm : public request audit Algorithm

1:Initialize: $V_l \leftarrow n_1, V_r \leftarrow n_{|P_{SD}|}, V_n = \{V_1 \ldots\ldots V_r\}$
2: while $|V_n| > 2$ do
3: audit (ni) = V [rand]
4: if $|X_i \cap X_s| \approx |X_s|$ then
5: $V_{l \leftarrow n_i}$
6: else
7: $V_r \leftarrow n_i$
8: end if
9: end while
10: return Vn

D. Secure multiple packet drop detection

The proposed system examines the case of multiple independently misbehaving nodes. There two strategies for the nodes: (a) continuous misbehavior, and (b) randomly alter between honesty and misbehavior. In either case, here show S can identify, isolate, and locate the misbehaving nodes. The first step is to identify that more than one misbehaving node exists in PSD, which is achieved.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

Prime fields are fields whose sets are prime. In other words, they have a prime number of members. Prime fields turn out to be of great use in asymmetric cryptography since exponentiation over a prime field is relatively easy, while its inverse, computing the logarithm, is difficult. Mathematically, a proof to this effect is neither known nor thought to be forthcoming. Before wide-scale implementation, it is thus of the utmost importance that an extensive investigation of the true complexity of the problem is done in order to obtain the highest degree of confidence in the security of discrete logarithm based cryptographic systems. Such an investigation is in progress by various researchers around the world.

KeyGen: Given the domain parameters (a,b,p,G,n,E) of an elliptic curve E over finite field Fp where p is a large prime that satisfy . Where G is the base point of order n, note that n*G = ∞, the private key x is randomly selected from [1, n-1], the public key is Y=xG, another point on the curve.

Encryption: Given the plaintext m and Y, output C
1. k ∈ [1, n – 1]
2. M = map (m)= mG
3. C= (R, S) = (kG, kY+mG)
Homomorphic operation: Given C1, C2... Cn, output C'
C'= (k1G, k1Y+m1G)+(k2G, k2Y+m2G)+…+(knG, knY+mnG)
C'= ((k1+k2+..kn)G, (m1+m2+mn)G+(k1+k2+..kn)Y)

Decryption: Given C' and the private key x, output m
1. M = S – xR
2. m =rmap(M)
The map function satisfies the desired additive homomorphic property. However, the reverse mapping function is the shortcoming of this scheme, the reverse function maps a given point M into a plaintext m, and thus, the ECDLP on M must be resolved.

V. EXPERIMENTAL RESULTS

During the simulation, each node starts its journey from a random spot to a random chosen destination. Once the destination is reached, the node takes a rest period of time in second and another random destination is chosen after that pause time. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. PDR is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source mobile node. It can be evaluated in terms of percentage (%).

Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node.

Average end-to-end delay Average end-to-end delay signifies how long it will take a packet to travel from source to destination node. It includes delays due to route discovery, queuing, propagation delay and transfer time.

TABLE I COMPARE PDR EXISTING WITH PROPOSED

Algorithms	**No of Nodes**						
	10	**20**	**30**	**40**	**50**	**60**	**70**
Existing	54	50	64	79	84	88	91
Audit based Technique	65	67	85	83	87	94	98

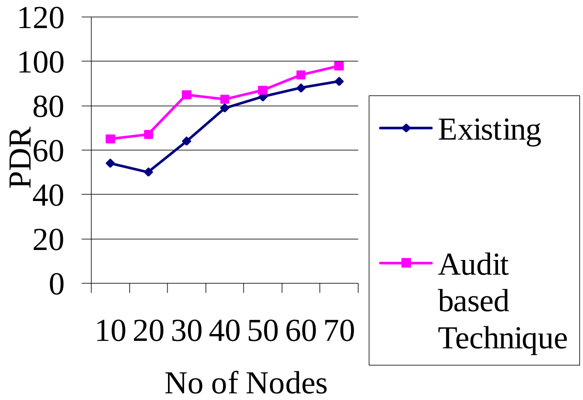

Fig. 2 Compare PDR existing with proposed

Shows packet delivery ratio against the number of nodes. It shows that the protocol has a better Audit method compare to existing.

TABLE III COMPARE THROUGHPUT EXISTING WITH PROPOSED

Algorithms	No of Nodes						
	10	20	30	40	50	60	70
Existing	5.1	6.4	7.5	8.2	8.7	9.1	9.5
Audit based Technique	5.8	6.9	7.6	9.1	10.3	11.7	12.4

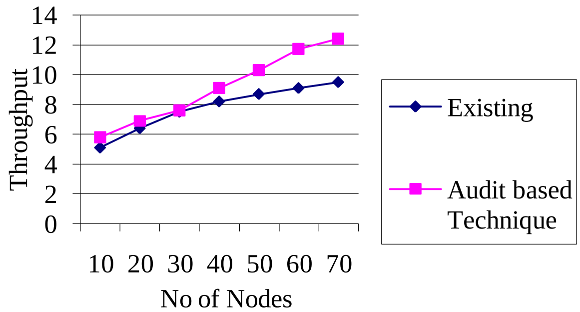

Fig. 3 Compare throughput existing with proposed

TABLE IIIII COMPARE END TO END DELAY EXISTING WITH PROPOSED

Algorithms	**No of Nodes**						
	10	**20**	**30**	**40**	**50**	**60**	**70**
Existing	5.8	4.1	3.2	3.1	2.8	2.5	2.1
Audit based Technique	4.1	3.2	2.7	2.1	1.9	1.2	0.5

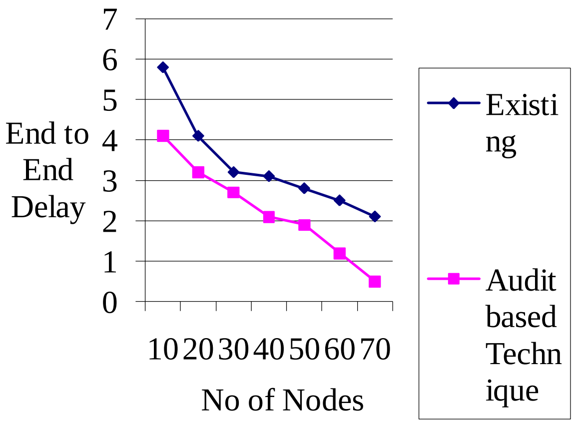

Fig. 4 Compare end to end delay existing with proposed

VI. CONCLUSIONS

Packet dropping attack which is a crucial issue in networks. Link error and malicious packet dropping are two sources for packet losses. While observing a sequence of packet losses in the network, it is difficult to identify whether the loss is due to link errors or malicious nodes. Packet may be dropped during forwarding of routing information or during data forwarding. Dropping can be due to presents of malicious nodes or due to link error. Hence to improve the detection accuracy, the correlations between lost packets is identified. The proposed method is based on detecting the correlations between the lost packets over each hop of the path. It 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 Audit based elliptic curve cryptography (AECC) which describes the status of each packet in a sequence of packet transmission. Therefore, by detecting the correlations between the lost packets, one can decide whether the packet loss is purely due to link errors, or is a combined effect of malicious drop and link error. Trust is used to identify the malicious node or not. The trust management in the WSN is like usually RREQ and RREP message passing between nodes. The energy is used to distinguish between altruism and selfish node. The future work plan to block-based HLA signature could be explored. Here will evaluate the effect of this method as our next step. Second, in this paper, we mainly focused on showing the feasibility of the proposed mechanism. The decision threshold used in the detection was obtained by trial-and-error. In our future work, we will study the optimization of this threshold. The impact of different topology remains an issue to be evaluated.

REFERENCES

[1] 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

[2] 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

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

[4] 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.

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

[6] 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.

BIOGRAPHIES

Parameswaran T has received his Bachelor's degree in engineering Electronics and Communication Engineering from Velalar College of Engineering and Technology, Erode in 2005 and Master of Engineering in Software Engineering from Anna University Guindy, Chennai in 2008. He is currently pursuing his PhD Anna University Chennai. He is currently working as Teaching Fellow in the department of Computer Science and Engineering in Anna University Regional Campus, Coimbatore, Tamilnadu, India.

Dr. C. Palanisawmy has received his Bachelor's degree in engineering Electronics and Communication Engineering from University of Madras, Chennai and Master of Engineering in Communication System (Gold Medallist) from Thiagarajar Collage of Engineering, Madurai, and Madurai Kamarajar University in 1998 and 2000 respectively, He has received his Ph.D from the faculty of Information and Communication Engineering, Anna University, Chennai in 2009. He has more than 13 years of academic and research experience and currently he hold the post of professor and Head of the Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam and TamilNadu, India. He has published more than 30 research papers in various journals and conference. He organized more than 10 workshops and holds 2 funded projects. He is life time member of ISTE.

Saranyadevi RD has completed her Bachelor's degree in engineering in Computer Science from Vickram Collage Engineering, Madurai Tamilnadu, India (2010) and presently pursuing Master of Engineering in the department of Computer Science and Engineering in Anna University Regional Campus, Coimbatore, Tamilnadu, India. Her research interests are wireless Ad Hoc networks.