2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)
August 28-29, 2018; Shahid Rajaee Teacher Training University - Tehran, Iran

A New Statistical Method for Wormhole Attack Detection in MANETs

Hossein As'adi
School of Elec. And Comp. Eng.
Shiraz University
Shiraz, Iran
hs.elcnet.1990@gmail.com

Alireza Keshavarz-Haddad
School of Elec. And Comp. Eng.
Shiraz University
Shiraz, Iran
keshavarz@shirazu.ac.ir

Ali Jamshidi
School of Elec. And Comp. Eng.
Shiraz University
Shiraz, Iran
jamshidi@shirazu.ac.ir

***Abstract*—Mobile ad hoc networks (MANETs) are a set of mobile wireless nodes that can communicate without the need for an infrastructure. Features of MANETs have made them vulnerable to many security attacks including wormhole attack. In the past few years, different methods have been introduced for detecting, mitigating, and preventing wormhole attacks in MANETs. In this paper, we introduce a new decentralized scheme based on statistical metrics for detecting wormholes that employs "number of new neighbors" along with "number of neighbors" for each node as its parameters. The proposed scheme has considerably low detection delay and does not create any traffic overhead for routing protocols which include neighbor discovery mechanism. Also, it possesses reasonable processing power and memory usage. Our simulation results using NS3 simulator show that the proposed scheme performs well in terms of detection accuracy, false positive rate and mean detection delay.**

Keywords—MANET, Wormhole attack, Statistical methods, number of neighbors, number of new neighbors, SWAN, NS3 simulator

I. INTRODUCTION

Network security is an intrinsic part in designing any network architecture. Wireless networks face more challenging tasks to solve these issues compared to their wired counterparts. Even more severe is dealing with security threats in multihop wireless networks such as wireless mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs), due to their specific properties including lack of infrastructure, dynamic topology, limited bandwidth and low battery power. In the past decade, many attacks have been introduced in the literature relating to multihop wireless networks. In this paper, we focus on a particularly devastating attack on multihop routing called *wormhole attack*.

The wormhole attack was first introduced independently by Hu et al. [1], Papadimitratos et al. [2] and Sanzgiri et al. [3]. It can be considered as a two-phase attack implemented by two attacker nodes. The first phase includes capturing packets at one location, sending them through a link called wormhole tunnel and replaying these packets there. Wormhole tunnel can be set up in several ways, e.g. directional long-range high-bandwidth wireless channel, wired link, optical link or virtual link through packet encapsulation. This (seemingly) faster channel can persuade legitimate nodes (whether truely or falsely) that routes through the tunnel are the most efficient. In fact, wormhole creates fake neighbors in the network, and thus, network topology changes. In the second phase attackers can exploit

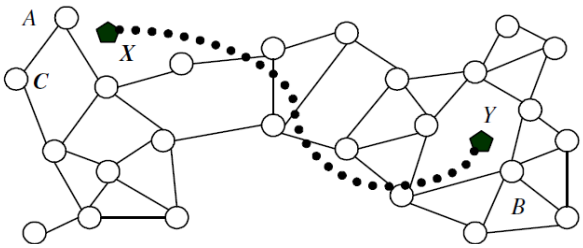

Fig. 1. Wormhole attack. The adversary controls nodes X and Y and connects them through a low-latency link [4].

the subsequent absorbed traffic whichever way they wish. These include (selectively) dropping packets that turns wormhole into a grayhole/blackhole, modifying or delaying packets, analyzing or recording traffic, turning the tunnel on and off periodically, etc. Fig. 1 shows a wormhole attack implemented by attacker nodes X and Y connected through a low-latency link.

Several classifications of wormholes have been proposed in the literature based on different properties of the attack. Khalil et al. [5] have divided wormholes into five categories based on how the tunnel is implemented: packet encapsulation, out-of-band channel, high-power transmission, packet relay and protocol deviations. In [6] and [7], classifications have been independently proposed, with different terminologies but identical in essence, in terms of whether wormhole nodes are visible on routes and according to them wormholes are either exposed/open or hidden/closed.

Since the discovery of wormhole attack in MANETs, different countermeasures have been proposed to prevent, mitigate or detect this devastating attack. Shin et al. [8] proposed a method to detect and isolate wormhole attacks in MANETs. The main idea is to create many possible routes when sending Route Request (RREQ) from source to destination and to use those routes as reference of each other, in order to find malicious nodes with suspicious behavior. Working in three steps, their method involves using routes redundancy, routes aggregation and calculating round-trip time (RTT) of all listed routes.

Jain et al. [9] proposed the use of a physical layer authentication scheme and secure neighbor discovery for the mitigation of wormhole attacks. They look for apparent channel noise due to replay and encapsulation performed by wormhole nodes.

Dhurandher et al. [10] proposed Energy-Efficient Scheme Immune to Wormhole attacks (E2SIW) protocol that

978-1-5386-7582-3/18/$31.00 ©2018 IEEE

uses the location information of nodes to detect the presence of a wormhole. The protocol is capable of detecting wormhole attacks employing either hidden or exposed nodes.

Fatehpuria et al. [11] presented a mechanism for prevention of wormhole attack and detecting the pinpoint location of wormhole, through observing the delay of different paths to receiver and verification of digital signature. It works for both hidden and exposed wormholes.

Chaurasia et al. [12] proposed a method to detect wormhole attack called Modified wormhole detection AODV protocol (MAODV). Detection is performed using number of hops in different paths from source to destination and delay of each node in different paths from source to destination.

Kim et al. [13] proposed a counterattack-detection scheme in transmission time-based wormhole detection methods to resist attackers who fabricate time stamps for a RREQ or RREP to evade these methods.

Patidar et al. [14] presented a hop count analysis approach to detect wormhole attacks along routes in ad hoc networks. The proposed technique makes use of variance in routing information between neighbors to detect wormholes. The wormhole-affected routes are distinguished from legitimate routes by analyzing the hop count value of all paths.

Sharma et al. [15] proposed a way to protect network from wormhole attack by using identity-based signature scheme on cluster-based ad hoc network.

Jamali et al. [16] proposed an improvement over AODV routing protocol to design a wormhole-immune routing protocol named Defending Against Wormhole Attack (DAWA). It defends against wormhole attack in two phases: In phase one, the system selects efficient routes using fuzzy logic; in phase two, it identifies the immune route among the selected routes using artificial immune system.

One category of countermeasures against wormhole attack, which is of more interest to us, is statistical methods. Song et al. [17] proposed a statistical solution in multi-path routing protocols called Statistical Analysis of Multi-path (SAM). The main idea of SAM is based on the fact that the wormhole links are selected for routing with abnormally high frequency, and by comparing with normal statistics, it can identify the wormhole links. Another method proposed by Buttyán et al. [18] captures the abnormal increase of number of neighbors and the decrease of the shortest path lengths due to wormholes in WSNs. The base station then centrally detects wormholes using hypothesis testing based on prestatistics of normal networks. Pham et al. [19] proposed a statistical approach to detect wormhole and localize placement of its endpoints in delay tolerant networks by making use of number of neighbors as detection parameter. The idea behind it is to compare number of neighbors of special nodes, called infrastructure nodes, in the current time to the average of number of neighbors already collected by them over a period of time. Song et al. [20] proposed a decentralized statistical algorithm for mobile wireless sensor networks (mWSNs) named Statistical Wormhole Apprehension using Neighbors (SWAN). It is an online lightweight approach to detect wormholes using the change in the statistics of number of neighbors for each node between the previous history, called a training set, and recent samples called a test set.

Our contribution in this paper is to continue the work done in [20] to improve the performance of SWAN algorithm in two steps. We first modify SWAN through applying changes to its decision rule and parameters and then present our proposed scheme by introducing and inserting a secondary statistical detection parameter to it. Similar to SWAN, our scheme lacks constraints existing in most countermeasures agaist wormhole attack such as high detection delay (e.g., because of taking action in the second phase of attack), creating traffic overhead, need for special hardwares, time synchronization among nodes or alteration of routing protocol, each of which limits their applicability in real networks. The proposed scheme is a decentralized lightweight solution that detects all categories of wormhole attack with considerably low detection delay and while the first phase of attack is being performed, the only requirement being that network routing protocol should include a neighbor discovery mechanism through the use of periodic messages (e.g., Hello packets). Also, it needs reasonable processing power and memory usage. Simulation results using NS3 simulator show that the proposed scheme outperforms SWAN.

The rest of the paper is organized as follows: Section II presents an overview of SWAN algorithm as the basis of our proposed work. The proposed scheme is explained in detail in Section III. Simulation and performance evaluation is presented in Section IV. Finally, conclusions and future work are outlined in Secion V.

II. A Brief Overview of SWAN

The idea behind SWAN approach is to use an online outlier detection algorithm based on *number of neighbors* for each node to detect wormholes. A sensor node receives beacon messages from neighboring sensors, and collects a recent history of its number of neighbors. As nodes move around the field, their number of neighbors will change over time. Once a sensor node encounters a wormhole, however, the number of neighbors is expected to increase beyond a range of statistical fluctuation. Thus, the task is to discover if the current or recent number of neighbors exhibit abnormal increases compared to the normal ones from outside of the wormhole (previous history). SWAN makes decisions of Wormhole Status (*WHS*; true or false) at the end of successive *time slots*. Therefore, the problem can be formulated as making decisions by each node in each time slot whether the distance between its previous data set of number of neighbors (training set) and recent data set of number of neighbors (test set) is greater than a threshold or not.

As SWAN is a statistical approach, the underlying distribution of number of neighbors in a sliding time window W must be estimated. To do that, SWAN has used kernel estimators. Then, by the aid of *Kullback-Liebler (KL) divergence*, the difference between training set (S_{train}) and test set (S_{test}) is computed and the decision of declaring Wormhole Status is made.

Each mobile node runs the SWAN algorithm to detect Wormhole Status on its movement. The SWAN maintains the most recent events of the number of neighbors by using sliding windows for regular training (W_{reg}) and testing (W_{test}).

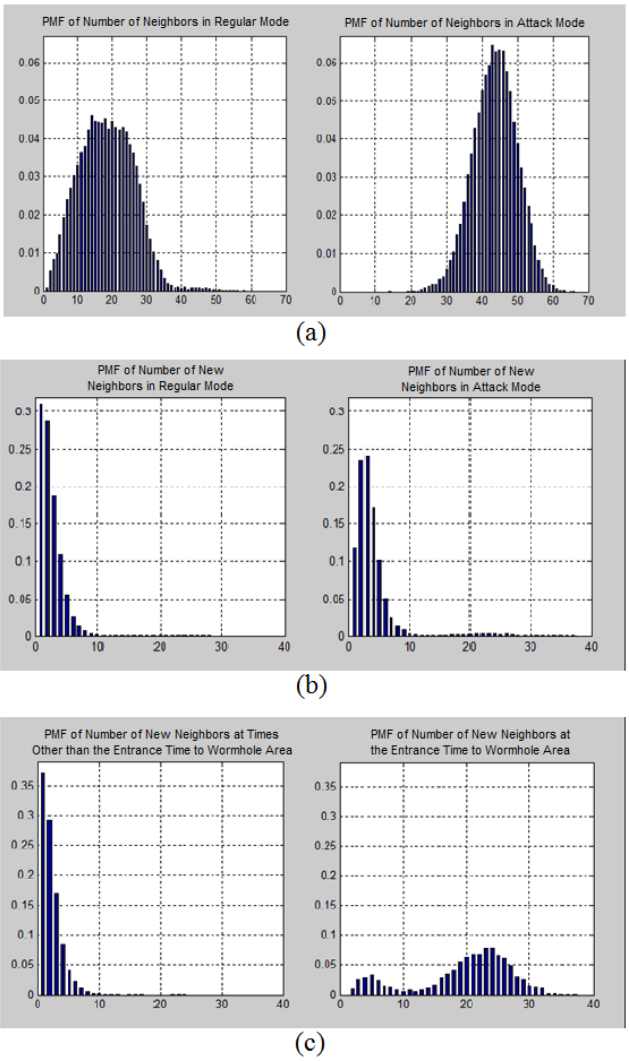

Fig. 2. (a) PMFs of number of neighbors in regular and attack mode; (b) PMFs of number of new neighbors in regular and attack mode; (c) PMFs of number of new neighbors at the entrance times and otherwise.

When a node is not in a wormhole area, it checks if the normalized distance between the distributions of the training (S_{train}) and test (S_{test}) sets is greater than a threshold. If so, it concludes the node entered into a wormhole area. The new W_{test} value is added to the wormhole sliding window W_{wh}. Otherwise, it updates the regular sliding window W_{reg} entries by removing the oldest elements and adding new entries with W_{test}. When a node is already in a wormhole area, it checks the exit condition by using the distance of distributions between the distributions of train (S_{train}) and test (S_{test}) sets. If it becomes less than the threshold, it concludes the node is not in a wormhole anymore. The W_{wh} entries are cleaned up and the W_{test} value is used to update the sliding window W_{reg}. Otherwise, it updates the W_{wh} entries by removing the oldest elements and adding new entries with W_{test} [20].

III. Proposed Scheme

In this section, we aim to propose a new statistical scheme based on SWAN algoritjm by changing it in the following ways:

1) applying small, yet efficient, changes to its decision rule, sliding time windows and data sets, and

2) adding a secondary detection parameter named *number of new neighbors*.

A. Applying Changes to Decision Rule, Sliding Time Windows and Data Sets

- S_{train} has been replaced by two constant training data sets S_{reg}, containing samples of number of neighbors in regular mode (when a node is not in wormhole area), and S_{wh}, containing samples of number of neighbors in attack mode (when a node is in wormhole area), while W_{reg} and W_{wh} are removed. Being constant prevents entering wrong data to S_{reg} and S_{wh} if the algorithm makes wrong decisions.
- The decision rule is composed of comparing the distance between S_{test} and S_{reg} with the distance between S_{test} and S_{wh}, instead of just comparing S_{test} with S_{train}, in order to eliminate the correlation between decisions of adjacent time slots.
- We call the algorithm obtained by applying the above changes "the modified SWAN".

B. Introducing a New Detection Parameter: Number of New Neighbors

We define number of new neighbors for each node as the number of neighbors added to neighbor list of a node in the current moment compared to the previous one. Therefore, if the set of a node's neighbors in time n is

$$S(n) = \{s_k\} \quad k = 1, 2, \ldots, K \tag{1}$$

then the set of the node's new neighbors in the same moment becomes

$$S_{new}(n) = \{s_k \in S(n) \mid s_k \notin S(n-1)\} \quad k = 1, 2, \ldots, K' \tag{2}$$

To the best of our knowledge, "number of new neighbors" has not been used before as a statistical parameter to defend against wormhole attack. To show that the proposed detection parameter can improve the algorithm, we must show that the probability mass functions (PMFs) of number of new neighbors in regular and attack modes have less overlap compared to those of number of neighbors, in general or under certain conditions, and as a result statistical decisions based on using number of new neighbors make less errors. So, first we investigate the difference between empirical PMFs of regular and attack modes for these two detection parameters without setting any conditions. As an example, consider PMFs of Fig. 2 obtained by using fifty thousands data points for each one and applying simulation parameters of Table II.

KL divergence of PMFs in Fig. 2(a) is 0.53 while the same parameter for PMFs of Fig. 2(b) is 0.45. So, if no condition is set, inserting number of new neighbors to the algorithm seems to be of no use. However, by taking a closer look at Fig. 2(b), it can be seen that PMF of attack mode has small values in the region between 17 and 27 which cannot be neglected. This corresponds to the exact time when a node enters a wormhole area. That being said, this time we construct PMFs of number of new neighbors under the following condition: one including number of new neighbors at the entrance times to wormhole area and the other relating

TABLE I. NOTATIONS

Notation	Meaning
S_{reg}	Training set containing samples of "number of neighbors" in regular mode (constant)
S_{wh}	Training set containing samples of "number of neighbors" in attack mode (constant)
$S_{entrance}$	Training set containing samples of "number of new neighbors" at the entrance time (constant)
S_{other}	Training set containing samples of "number of new neighbors" at times other than entrance time (constant)
S_{test}	Test set containing samples of "number of neighbors"
$S_{test}2$	Test set containing samples of "number of new neighbors"
Dist()	Function which computes distance (KL divergence) between its input arguments
W_{test}	Sliding time window maintaining recent samples of "number of neighbors"
$W_{test}2$	Sliding time window maintaining recent samples of "number of new neighbors"
K_{test}	Length of the window W_{test}
$T_{sh}1$	Threshold value relating to "number of neighbors"
$T_{sh}2$	Threshold value relating to "number of new neighbors"
WHS	Wormhole status of a node, True or False

to number of new neighbors in other moments, i.e., when a node is already in a wormhole area or node is not in a wormhole area. The resulting diagram is depicted in Fig. 2(c). Now the KL divergence of PMFs increases to 0.56.

The "number of new neighbors" parameter has the following properties:

- It works best when the entrance time to a wormhole area is concerned (and hence reducing mean detection delay).
- It can only detect entrance to wormhole areas; otherwise it cannot make any decision.
- By taking the previous two properties into account, it can be concluded that number of new neighbors cannot be used in an algorithm independently. The best practice is to integrate this parameter as a secondary detection parameter alongside a primary one, such as number of neighbors, to improve an already-proven algorithm.

Therefore, a second decision rule and new data sets, sliding windows and parameters relating to number of new neighbors (listed in Table I) are added to the modified SWAN algorithm to form the proposed algorithm (Algorithm 1).

Each mobile node runs the proposed algorithm in each time slot of length K_{test} to detect wormhole. Decisions made in non-overlapping time slots are independent from each other. The reader is encouraged to see Table I before proceeding further. The proposed algorithm works as follows: Test sets S_{test} and $S_{test}2$ of the current time slot are created using W_{test} and $W_{test}2$. The first decision rule is related to the "number of new neighbors" parameter. It compares the distance (KL divergence) between PMFs (estimated by a kernel estimator) corresponding to $S_{test}2$ and training set $S_{entrance}$ with $S_{test}2$ and training set S_{other}. If the first distance multiplied by a threshold ($T_{sh}2$) is greater than the second, it is concluded that the node has entered a wormhole area and *WHS* becomes true. Otherwise, number of new neighbors cannot make any decisions and the other decision rule is applied. It decides the same way as the first rule, of course by making use of "number of neighbors"

Algorithm 1 *Proposed Algorithm*

$S_{test} = W_{test}$.Update (K_{test})
$S_{test}2 = W_{test}2$.Update (K_{test})
if ($T_{sh}2 \times$ Dist (S_{other}, $S_{test}2$) < Dist ($S_{entrance}$, $S_{test}2$)) **then**
  WHS = true
else
  if ($T_{sh}1 \times$ Dist (S_{reg}, S_{test}) < Dist (S_{wh}, S_{test})) **then**
    WHS = false
  else
    WHS = true
  end if
end if

parameter and its relating data sets (S_{test}, S_{reg} and S_{wh}) and threshold (T_{sh}), with the only difference being that it can also declare *WHS* as false. It must be noted that eliminating the first decision rule in the proposed algorithm yields modified SWAN.

IV. SIMULATION AND PERFORMANCE EVALUATION

In this section we evaluate our proposed algorithm based on three performance metrics: *detection accuracy*, *false positive rate* and *mean detection delay*. Detection accuracy is the ratio of number of time slots including wormhole attack, in which attack is correctly detected, to the number of all time slots in a simulation. False positive rate is the ratio of number of time slots without wormhole attack, in which attack is incorrectly detected, to the number of all time slots in a simulation. Detection delay is the time between occurance of an attack and its detection. By averaging this parameter over all existing test data, mean detection delay is computed. Furthermore, a time slot including wormhole attack is the one containing at least one moment of attack. The simulations are carried out using NS3 simulator [21]. The simulation parameters used are listed in Table II. The information of all the nodes are gathered to calculate the above metrics. The window length in all the tests (except the window length test) is set to 10. We investigate the impact of window length (K_{test}), node density and radio range of nodes on detection accuracy and mean detection delay of the

TABLE II. SIMULATION PARAMETERS

Simulation Time	1000s
Simulation Repetition	10
Network Dimensions	500m×500m
Number of Nodes	150,200,250,300,350,400
Radio Range	40m,45m,50m,55m,60m,65m,70m
Antenna	Omnidirectional
Wireless Channel Capacity	54 Mb/s
MAC Protocol	802.11
Routing Protocol	AODV
Traffic	UDP-CBR
Packet Size	512 bytes
Data Rate	5 kb/s
Mobility Model	Random Waypoint
Maximum Node Speed	20 m/s
Maximum Pause Time	0s
Number of Wormhole Nodes	2
Wormhole Type	Wired Out-of-Band
Wormhole Link Capacity	500 Mb/s
Wormhole Mobility Model	Constant
Positions of Wormhole Endpoints	(150,150) & (350,350)
Sampling Period of "Number of (New) Neighbors"	1s

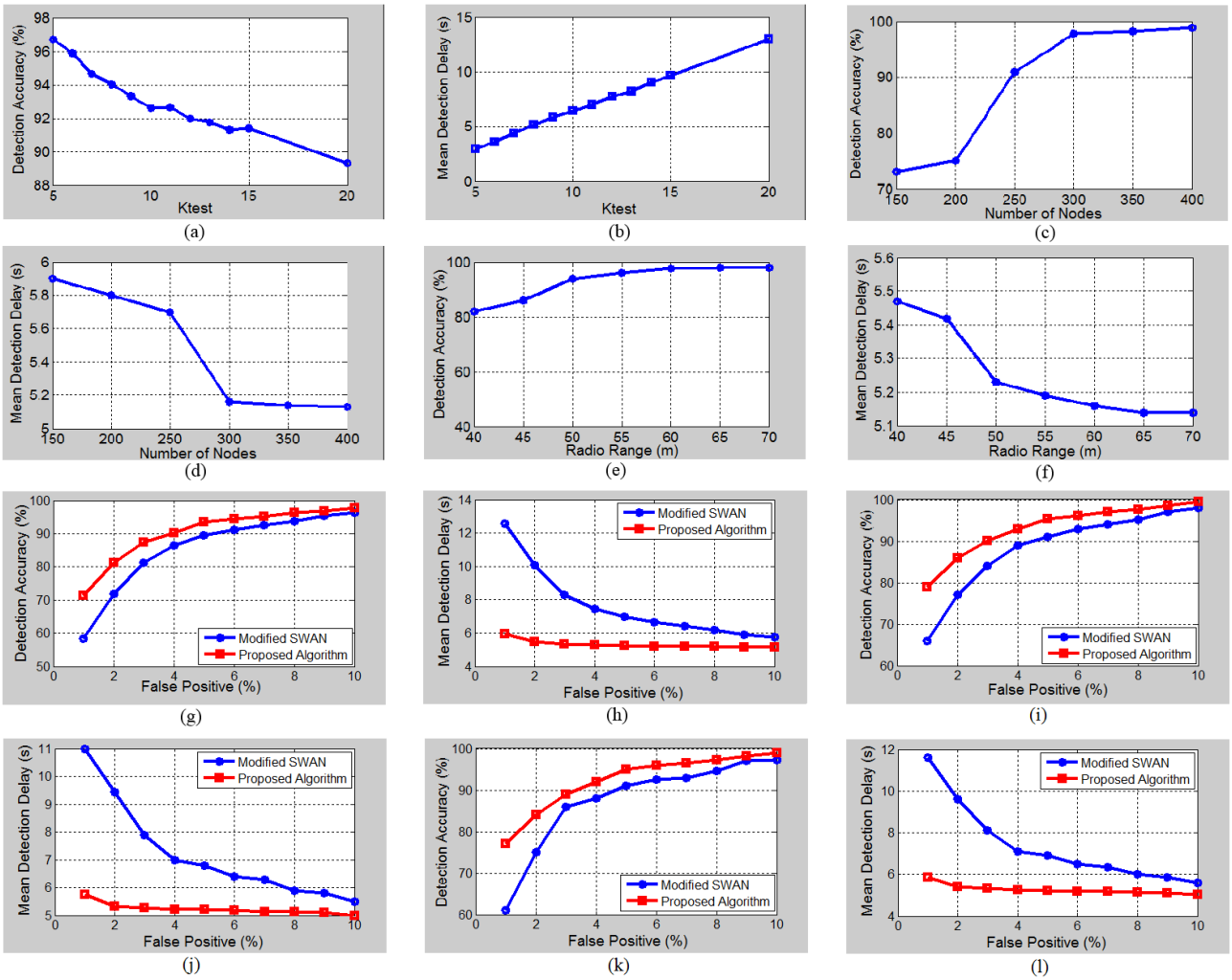

Fig. 3. (a) Detection accuracy vs. K_{test} (FPR = 10%, node density = 300, radio range = 60m); (b) Mean detection delay vs. K_{test} (FPR = 10%, node density = 300, radio range = 60m); (c) Detection accuracy vs. number of nodes (FPR = 10%, K_{test} = 10, radio range = 60m); (d) Mean detection delay vs. number of nodes (FPR = 10%, K_{test} = 10, radio range = 60m); (e) Detection accuracy vs. radio range (FPR = 10%, K_{test} = 10, node density = 300); (f) Mean detection delay vs. radio range (FPR = 10%, K_{test} = 10, node density = 300); (g) Detection accuracy vs. FPR (K_{test} = 10, node density = 300, radio range = 60m); (h) Mean detection delay vs. FPR (K_{test} = 10, node density = 300, radio range = 60m); (i) Detection accuracy vs. FPR (K_{test} = 10, node density = 400, radio range = 60m); (j) Mean detection delay vs. FPR (K_{test} = 10, node density = 400, radio range = 60m); (k) Detection accuracy vs. FPR (K_{test} = 10, node density = 300, radio range = 70m); (l) Mean detection delay vs. FPR (K_{test} = 10, node density = 300, radio range = 70m)

proposed algorithm for a fixed false positive rate of 10%. With the change of the above three parameters in each test, different training sets (containing sample values relating to the test) must be applied to the algorithm. We also compare detection accuracy and mean detection delay of the modified SWAN and the proposed algorithm for equal values of false positive rate. Each test has been run for 1000s and repeated 10 times. It is important to note that SWAN has been proposed in [20] just as an idea and without presenting any experimental results. Hence, we compare our proposed algorithm with modified SWAN.

Fig. 3 shows the results of detection accuracy, false positive rate and mean detection delay of the proposed algorithm with varying window lengths, node densities and radio ranges. It also illustrates the impact of integrating number of new neighbors in the proposed algorithm. Fig. 3(a) shows the relation between accuracy and K_{test} for false positive rate of 10%, radio range of 60m and 300 mobile nodes. The accuracy declines as K_{test} increases. The reason lies in decrease of accuracy in windows including start or end of attack. The number of samples regarding presence of attack in these windows compared to window length gets smaller and as a result, affects the probability of detection. Moreover, mean detection delay increases as K_{test} goes up. The increase in window length practically leads to higher detection delays, because algorithm decisions are made only at the end of time slots (Fig. 3(b)).

The impact of node density on algorithm performance is depicted in Fig. 3(c) for false positive rate of 10%, window length of 10 and radio range of 60m. Higher node densities cause more Hello packets to be sent through wormhole and consequently making PMFs in regular and attack modes of both detection parameters more separate which rises the detection accuarcy. As a consequence, mean detection delay augments, too, because probability of detection in windows including the start of attack increases (Fig. 3(d)).

Variations of radio range of nodes have the same effect on results as node density. Higher radio ranges mean more Hello packets going through the tunnel and hence more number of (new) neighbors. Impact of radio range on detection accuracy and mean detection delay for false

positive rate of 10%, window length of 10 and node density of 300 is demonstrated in Figs. 3(e) and (f).

Figs. 3(g), (h), (i), (j), (k) and (l) show how "number of new neighbors" parameter improves the algorithm for different values of radio range and node density. In fact, adding this parameter increases probability of detection in windows including start of attack (the value of which was average in its absence). Improvement of acuuracy and mean detection delay for high false positive rates becomes less significant because "number of neighbors" parameter is already working well in this condition. These figures in fact illustrate the difference in performance of modified SWAN and our proposed scheme.

V. Conclusions and Future Work

Wormhole attack is one of the most challenging attacks to detect in MANETs to date. In this paper, we proposed a statistical scheme to detect such an attack. It incorporates an online, lightweight and decentralized algorithm that detects attackers while the first phase of attack is being performed, does not create any traffic overhead and eliminates constraints observed in most previous solutions. Also, it possesses reasonable processing power and memory usage. We proposed our scheme in two steps. First, we modified SWAN, the scheme it is based on, through applying changes to its decision rule and parameters and then inserted a secondary statistical detection parameter to it. Proposed scheme makes use of two statistical parameters: number of neighbors and number of new neighbors. We showed by performing simulations that our method outperforms SWAN in terms of detection accuracy, false positive rate and mean detection delay. We found that the robustness of our scheme depends upon node density and radio range of nodes in the network beside window length of the algorithm. Future work includes evaluating and enhancing our scheme in difficult conditions that make statistics in regular and attack modes less different (such as non-uniform mobility models, sparse networks and smart wormholes) and applying "number of new neighbors" parameter as a secondary detection parameter to other statistical solutions.

References

[1] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), 2003, pp. 1976–1986.

[2] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation, 2002, vol. 31.

[3] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in Proc. IEEE ICNP, 2002, pp. 78–87.

[4] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Network and Distributed System Security Symposium (NDSS), 2004, vol. 4, pp. 241–245.

[5] I. Khalil, S. Bagchi, and N. B. Shroff, "Liteworp: A light-weight countermeasure for the wormhole attack in multihop wireless networks," in Proc. DSN, 2005, pp. 612–621.

[6] H. S. Chiu and K. S. Lui, "DELPHI: wormhole detection mechanism for ad hoc wireless networks," 1st International Symposium on Wireless Pervasive Computing, 2006, pp. 6–11.

[7] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks," Wireless Commun. Mobile Comput., vol. 6, pp. 483–503, 2006.

[8] S. Y. Shin and E. H. Halim, "Wormhole attacks detection in MANETs using routes redundancy and time-based hop calculation," International Conference on ICT Convergence (ICTC), 2012, pp. 781–786.

[9] S. Jain and J. S. Baras, "Preventing wormhole attacks using physical layer authentication," in Proceedings of the 2012 IEEE Wireless Communications and Networking Conference (WCNC), 2012, pp. 2712–2717.

[10] S. K. Dhurandher, I. Woungang, A. Gupta, and B. Bhargava, "E2SIW: An energy efficient scheme immune to wormhole attacks in wireless ad hoc networks," Proc. of the WAINA Workshop, Fukuoka, Japan, 2012, pp.472–477.

[11] A. K. Fatehpuria and S. Raghuwanshi, "An efficient wormhole prevention in MANET through digital signature," International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 3, 2013.

[12] U. K. Chaurasia and V. Singh, "MAODV: Modified wormhole detection AODV protocol," in 2013 IEEE Sixth International Conference on Contemporary Computing (IC3), 2013, pp. 239–243.

[13] D. Kim, H. Kim, G. Kim, and S. Kim, "A counterattack-detection scheme in transmission time-based wormhole detection methods," Hindawi Publishing Corporation-International Journal of Distributed Sensor Networks, vol. 9, no. 3, 2013.

[14] K. Patidar and V. Dubey, "Modification in routing mechanism of AODV for defending blackhole and wormhole attacks," in IEEE Conference on IT in Business, Industry and Government (CSIBIG), 2014, pp. 1–6.

[15] D. Sharma, V. Kumar, and R. Kumar, "Prevention of wormhole attack using identity based signature scheme in MANET," Computational Intelligence in Data Mining, vol. 2, pp. 475–485, 2016.

[16] S. Jamali and R. Fotohi, "DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system," in the Journal of Supercomputing, vol. 73, no. 12, pp. 5173–5196, 2017.

[17] N. Song, L. Qian, and X. Li, "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach," in Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, 2005, pp. 8–15.

[18] L. Buttyán, L. Dóra, and I. Vajda, "Statistical Wormhole Detection in Sensor Networks," Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS), Visegrád, Hungary, 2005, pp. 128–141.

[19] T. N. D. Pham and C. K. Yeo, "Statistical wormhole detection and localization in delay tolerant networks," in Proc. IEEE 11th Consum. Commun. Netw. Conf. (CCNC), 2014, pp. 380–385.

[20] S. Song, H. Wu, and B. Choi, "Statistical ormhole detection for mobile sensor networks," in ICUFN, Conference on Ubiquitous and Future Networks, 2012, pp. 322-327.

[21] NS3. www.nsnam.org/.