A Review on Trust Based Method to Detect Black Hole Attack in Manet

Priyanka Donga[1], Shraddha Joshi[2]

Marwadi Education Foundations, Group of Institutions, Rajkot, Gujarat, India[1, 2]

Abstract: Self configuring nature of MANET exposes itself to variety of active and passive attacks. Black hole attack is an active attack which creates disruption in communication path. There are two types of black hole attack i.e. single black hole attack and collaborative black hole attack. We have considered single black hole attack. In this research work, single malicious node doesn't allow the transmission of legitimate packets to the receiver and drop that packet. In this work in trust we present a detailed survey on various trust computing approaches and this approaches are used find the black hole attack in MANET.

Keywords: Network Security; MANET; Effects; Black hole attack; trust

I. INTRODUCTION

Mobile ad-hoc network (MANET) is an infrastructure less dynamic network consist of wireless mobile nodes which communicate with each other without the use of any centralized authority. Due to its dynamic and infrastructure less nature it can be easily deployable and self organized for various applications such as [1]

1) Personal area networking using cell phone, laptop.
2) Military environment monitoring and communication.
3) Civilization environment likes taxi cab network, meeting rooms, sports stadiums.
4) An emergency operation likes search and rescue.

To develop various application of MANET different type of routing protocols are required which are elaborately discuss in [2-4] such as AODV (Ad hoc on demand distance vector routing protocol), DSR(Dynamic source Routing protocol), DSDV(Destination Sequences Distance Vector), ZRP(Zone Routing protocol).Our focus on AODV Routing protocol [2]. Due to self organizing and self configuring nature of mobile ad hoc network is prone to various kind of attack. In which black hole attack most prominent attack which affects the network performs. Black hole attack is one of the type of packet dropping attack. In the black hole attack are two types: 1) Single black hole attack 2) collaborative black hole attack. The black hole attack behaviors not properly and to drop all legitimate packets and also it sent fake reply to the source [5]. Trust based method focuses on finding trust value. Which is calculated based on the previous experience, opinion and performance of various network parameter receivers from the neighboring nodes. Through the trust value we can easily eliminate malicious node, can have minimum overhead and proper access control. Hence it can establish a best routing path between source and destination [6]. We organized this review paper by keeping in mind the various trust methods used to detect black hole attack. Section II discusses definition, properties and metrics that are used to compute trust to detect black hole attack in various existing literature. Section III summarization different trust based approaches available to compute trust value. Section IV discuses how the trust values are used to find the black hole attack in MANET. Section V is analysis of papers. Future research opportunities on trust and concluding remarks are given in Section VI.

II.TRUST DEFINITION, PROPERTIES, METRICS

A. Definition

Trust is abstract concepts it can't be define to the single context since combine many complex factors. In the case of mobile ad hoc network trust can be define as the reliance of network node on the ability to forward packet based on evidence generated by the performance of previous interaction in any mobile ad hoc network. In general we can categories trust in three types:
1) Direct trust 2) Indirect trust 3) hybrid trust
1) Direct trust: Direct observation on two malicious behaviors such as [6]: dropping packets and modifying the packets. It is based on the network sensing and it can directly measured by the immediate neighbors. In which the each observed node can forwarded packet to each observer and compare with the original packets. So it can identify the malicious behaviors of observe node. Then observer node observes is neighbor nodes and store its value. Direct trust is referring to the past behavior. Past behavior is most important in trust calculation [7].

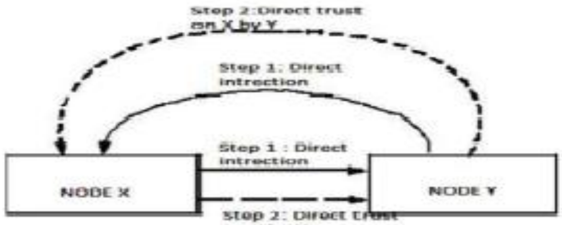
Step 2:Direct trust on X by Y
Step 1: Direct intrection
Step 1 : Direct intrection
NODE X
NODE Y
Step 2: Direct trust on Y by X

Fig 1: Direct trust

Direct trust calculation in using below equation [8]:

$$\text{Direct trust} = w1 * HT_d + w2 * CT_d \qquad (1)$$

Where W1+W2=1, HT(history of trust is ratio of number of packet forwarded and number of packet forwarded to) and CT (current trust is ratio of current node forwarded packet and current node forwarded packet to other node)

2) Indirect trust: Trust relationship on nodes is established on only recommendations. In which this evidence from the neighbor nodes are useful because it is judging the trustworthiness of the observed node. Then collecting the neighbor information and justify the nodes [6].

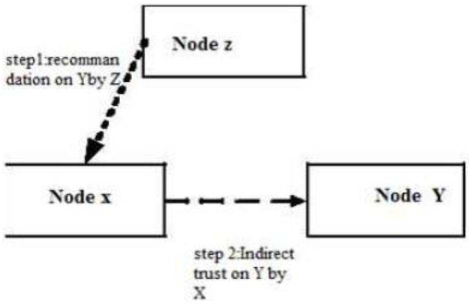
Node z
step1:recomman dation on Yby Z
Node x
Node Y
step 2:Indirect trust on Y by X

Fig 2: Indirect Trust

In above Fig 2 node z recommendation for trustworthy node of itself from source node x. Source node x finds trustworthy path between intermediate nodes Y.

Indirect observation calculation in using following [9]:

$$T_{AB}^{N} = m_{j1}(H) \oplus m_{j2}(H) \ldots\ldots \oplus m_{jn}(H) \qquad (2)$$

Where T_{AB}^{N} is indirect trust, H is Hypothesis, ji is node ($1 \leq i \leq n$), $m_{j1}(H)$ is probability value.

3) Hybrid trust: Hybrid trust is combination of direct trust and indirect trust. In this case first is source node direct interaction to any other node then node Z send to the recommendation for the node X. In last is node X send to trust value by node Y [6].

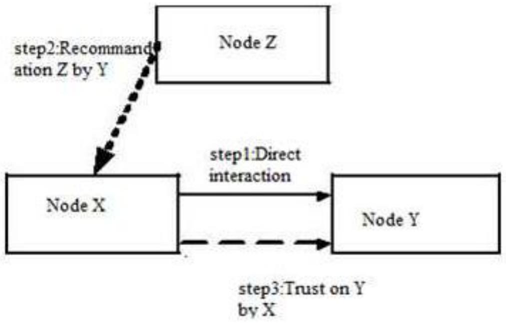

Fig 3: Hybrid Trust

Hybrid trust calculation in using following equation [6]:

$$Tx,y = \alpha Ts + \beta To \qquad (3)$$

Where Tx,y is node x trust on node y.α+ β= 1 such as α and β are constants. Ts is Compute by directly monitoring y for total packets dropped by y, packet forwarding delay by y, packets misrouted by y($0 \leq Ts \leq 1$).T_o is collective trust evolution by all other nodes on y ($0 \leq To \leq 1$).

B. Trust properties

Subjectivity: In MANET environment, subjectivity that Means right observation of node to find the trust of an observed node. Than different observer nodes it may have different trust values of same observed node. So, it dynamically was changing network topology [6].

Dynamicity: In this case trust node can be changed depending upon the node behaviors. It cannot static trust establishment in MANETs and given spatially local information [6].

Non transitivity: It means that, if node A trusts to node B then node B trust to node C but node A does not necessarily trust to node C [6].

Context dependence: It is based on the node behavior. For example if node A may trust B as a give fake reply but not as regular.

C. Metrics

1) Packet Delivery Ratio: The ratio between number of receiving packets and number of sending packets [8-9].

2) Over head: This metric describes how many routing packets for route discovery and route maintenance need to be sent to propagate the data packets [8].

3) Throughput: The total size of data packets successfully received by a destination node every second [8][9].

4) Threshold value: In [7][8] describe threshold base approaches measure trust value. If trust value is greater than threshold value then node is consider as trustworthy.

5) Trust Facts: Some approaches are used belief, disbelief and uncertainty function. In [6][9] dumpster shapher theory measure only [0,1] interval.

III. SUMMARIZATION DIFFERENT TRUST BASED APPROACHES AVAILABLE TO COMPUTE TRUST VALUE.

The author Chuanhao Qu et al. [7] has described Trust management mechanism used by light weight trust based on demand multipath protocol. It can be considered as the network node on the ability to forward packets or offered service timely, integrally and reliably.

There are two methods of Trust model as direct trust and indirect trust. Direct trust (DT) approach clouds reduce the buffer size and alleviate the computation overhead in this case the FT is packet forward to and FD means packet forwarded count every neighbor node. In which two factor used one is history trust value (HT) and second current trust value (CT) following below equation (4),(5),(6).

$$HT_d = \frac{\sum_{i=t-k}^{t} FD_d^i}{\sum_{i=t-k}^{t} FT_d^i} \qquad (4)$$

$$CT_d = \frac{FD_d^t}{FT_d^t} \qquad (5)$$

$$\mathrm{DT_d} = \omega 1 \times \mathrm{HT_d} + \omega 2 \times \mathrm{CT_d} \qquad (6)$$

Where ω1 and ω2 are assume.
Indirect trust (IT) is considering a malicious node can drop packets received from specific neighbor. It is periodically one hop broadcast and evolution to the neighbor. In this case node has $\mathrm{N_d}$ neighbors that have evaluated to the node d following equation (7) and (8).

$$\mathrm{TT_{d,i}} = \begin{cases} 1, \mathrm{if DT_d} \text{ of neighbor } i < \mathrm{THRESHOLD} \\ 0, \text{otherwise} \end{cases} \qquad (7)$$

$$\mathrm{IT_d} = \frac{\sum_{i=0}^{n-1} \mathrm{TT_{d,i}}}{\mathrm{N_d}} \qquad (8)$$

Comprehensive node trust (NT) is based on a threshold value in direct and indirect comparison and describes paper [5] following equation

$$\mathrm{NT} = \begin{cases} \mathrm{THRESHOLD}, \text{if } \mathrm{IT} > \mathrm{MIN_{VOTE}} \text{ and } \mathrm{DT} > \mathrm{THRESHOLD} \\ \mathrm{DT}, \text{otherwise} \end{cases} \qquad (9)$$

Then computation of path trust (PT) is finding the minimum link trust value. In this case routing path p, nodes n. Node represented by sequence N1, N2, N3..,Nn and Ni denotes the i^{th} node in the sequence Following equation (10).

$$\mathrm{PT_p} = \min\{\mathrm{NT1}, \mathrm{NT2}, \ldots\ldots, \mathrm{NTn}\} = \min\{\mathrm{NT_i}\} \quad (10)$$

The author Zhenxicng Wei et al. [8] OLSRv2 (optimized link state routing protocol version 2) In Trust management two components are used, one is trust from direct observation and second is trust from indirect observation. Direct observation from the observe node in which trust value is derived from Bayesian method. Indirect observation is obtaining the neighbor node of observe node and it is used the Dempster-Shafer theory (DST).Trust value evaluate is follow:

$$\mathrm{T} = \lambda \mathrm{T^s} + (1-\lambda)\mathrm{T^N} \qquad (11)$$

Where $\mathrm{T^s}$ is direct observation, $\mathrm{T^N}$ is indirect observation, λ is weight assign (0≤ λ ≤1). In trust evaluation with Direct Observation of two malicious behaviors available for dropt the packets and modifying packets. Direct observation assume each observe can over here packet forward by an observed node and compare with the original packets so, it can identify the malicious behavior of the observe node. It is used in the probability based on Bayesian method. In which calculate the observed node A and an observed node B following equation:

$$\mathrm{T_{AB}^{s}} = \rho \mathrm{T_{AB}^{D}} + (1-\rho)\mathrm{T_{AB}^{C}} \qquad (12)$$

Where $\mathrm{T_{AB}^{s}}$ is direct observation trust value, $\mathrm{T_{AB}^{D}}$ is trust value based on data packets, $\mathrm{T_{AB}^{C}}$ is control packets. ρ Is weight for data packets (0≤ ρ ≤1).

Trust Evaluation with Indirect Observ(5)ion refers to the DST method. It will introduce the theory of Belief Functions. This observation is more than one neighbor node between an observer and an Observed node when evaluating the DST.

The belief function based on two ideas: first degree of Belief about a proposition can obtain from subjective probability of a related and second these degree beliefs can be combined to gather on the condition that it is independence evidence. Indirect observation following:

$$\mathrm{T_{AB}^{N}} = \mathrm{m_{j1}(H)} \oplus \mathrm{m_{j2}(H)} \ldots\ldots \oplus \mathrm{m_{jn}(H)} \qquad (13)$$

Where $\mathrm{T_{AB}^{N}}$ is indirect trust, H is Hypothesis, ji is node (1≤ i ≤n), $\mathrm{m_{j1}(H)}$ is probability value.

Kannan Govindan et. al. [6] has explained that survey on various trust computing approached and comparison the trust computing approaches. In this paper manly three approaches available.
1) Direct trust: based on the experience component of trust for each node is directly measured by their immediate neighbor and update at regular interval in the trust table.
2)Indirect trust: based on the recommendation component for trust every node monitors its one hop neighbor nodes and generate trust report based on the neighbor nodes behavior.
3) Hybrid method: it is combination of the direct trust and indirect trust.

IV. BLACK HOLE DETECTION SYSTEMS

B. Light-Weight Trust-Based On-Demand Multipath Routing Protocol

Chuanhao Qu et.al [7] shows that Trust evidence theory using the established the light weighted trust based multi path routing protocol. It is extended the AMODV to LWT-AOMDV (light weighted trust based multi path routing protocol).
Proposed protocol is established multiple trustworthy paths when detecting path with malicious nodes. Several different experiments were conducted to compare these protocols. This paper aim reduces the overhead, maintains trust value and finding trust worthy node.

C. Trust management scheme

Zhexiong Wei et. al.[8] has described that Trust management scheme in two component used first is trust from direct observation and second is trust from indirect observation .The direct observation from an observer node then trust value is derived using Bayesian interface method.

The indirect trust is neighbor node of the observer node and trust value defines the Dempster- Shafer theory. Combining two components in the trust model and finding the trust value. Main aim, through put and packet delivery ratio is improved.

DOI 10.17148/IJARCCE.2016.56162

D. Intrusion Detection Systems

M.-Y. Su et. al.[9] has design as Intrusion detection system to detect and prevent selective black hole nodes. In which they have used anti black hole mechanism function to find the Trust value.

This value is used for node according to the normal difference between the routing messages transmitted from the node. Then comparing the threshold value and informing all nodes on the networks.

E. Triangular encryption

N. Chatterjee et. al. [10] has explained that Triangular encryption technique is basis of structure that is formed out of the source as well as different intermediate and final block of bits during the process of bits encryption. This paper is simulates the behavior of the black hole node in AODV.

E. Intrusion Detection &Prevention Approaches

Adnan Nadeem et. al. [11] shows In this paper survey intrusion detection and prevention mechanisms there are three approaches used. 1) ABID(Anomaly –based intrusion detection) it is based on the behavior based intrusion detection.

ABID First establishes a normal expected behavior and then compare the current behavior. 2) KBID(Knowledge-based intrusion detection) it is maintain a knowledge based looks for these pattern in an attempt to detect .3) SBID(specification based intrusion detection system) it is first define specification as set of constrains.

V. ANALYSIS

TABLE 1: ADVANTAGES, DISADVANTAGES, OBSERVED PARAMETERS, PARAMETERS VALUES OF EXISTING PAPERS

Reference No	Advantage	Disadvantage	Observed Parameter and Parameter value
[6]	No single point failure	Recommendation based trust is some time node generates false report.	Time Transmission range:180 m, Packet size:512 bytes, Data rate:2mbps
[7]	Update to maintain the path trust.	Decrees packet delivery ratio	Trust value, Mobility type, Channel capacity Channel time out:100s, Mobility change interval:5s,
[8]	High packet delivery ratio.	It can lower the trust of attack when misbehaves	Mobility type, Time, Packet size :512 bytes, Data rate:2 Mbps, Simulation time:300s
[9]	Low memory consumption	• Continuous transmission of routing message would lead to congestion of network. • Quickly establishing node. • IDS nodes cannot broadcast validate block message.	Coverage area, Mobility, Time Transmission range:250m, Pushtime:0,5,10,15s, Simulation time:500s, No of nodes:50
[10]	Low computation overhead.	• Very slow as the number of nodes increases. • Large Number of packet loss.	Packet, Percentage of packet received No. of nodes: 20
[12]	• ABID systems can early warning of potential intrusion in the network. • KBID is very low false positive rates.	• It generates false alarm. • Knowledge base method is detect only attack using the signature or patterns based	Identifier of the node, Trust value, Packet, Coverage area

DOI 10.17148/IJARCCE.2016.56162

VI. CONCLUSION AND FUTURE

The target objective of this research is single black hole attack using indirect trust method in MANET. The current scenarios resolve these problems of throughput, Packet delivery ratio and trust value. In these research works, issues are packet drop, decrease throughput value, decrease PDR value etc., due to malicious node and because of that accurate trust value can't be obtained. So in this regards, the present work includes completion of theoretical analysis.

The trust scheme is no single solution. There is wide range of applications present and many types of mechanisms available. A general observation is that so far, the existing research work lacks completeness.

REFERENCES

[1] I. Chlamtac, M. Conti and J.J.N. Liu, "Mobile ad hoc networking: imperatives and challenges".,Ad hoc networks, vol.1, no.1, pp.13-64, 2003.

[2] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A Review of Routing Protocols for Mobile Ad Hoc Networks", Ad Hoc Networks, vol. 2, pp.1-22, 2003.

[3] Daxesh N. Patel, Sejal B. patel, Hemangi R. Kothadiya and Pinakin D. Jethwa, "A Survey of Advance Secure RoutingProtocols in MANET", ICICES, vol. 2, no. 3, pp. 1-22, 2013.

[4] B. Kannhavong,H. Nakayama,Y. Nemoto,N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks". Wireless communications, IEEE, vol.14, no.5, pp.85-91, 2007.

[5] F.H. Tseng, L.D. Chou, and H.C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," Human-centric Comput. Inf. Sci., vol. 1, no. 1, pp. 1-16, 2011.

[6] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," IEEE Commun. Surv. Tutorials, vol. 14, no. 2, pp. 279–298, 2012.

[7] C. Qu, L. Ju, Z. Jia, H. Xu, and L. Zheng, "Light-Weight Trust-Based On-Demand Multipath Routing Protocol for Mobile Ad Hoc Networks," 2013 12th IEEE Int. Conf. Trust. Secur.Priv. Comput. Commun., pp. 1–8, 2013.

[8] Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning," IEEE Trans. Veh. Technol., vol. 63, no. 9, pp. 1–12, 2014.

[9] M.Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Computer Commuication., vol. 34, no. 1, pp. 107–117, 2011.

[10] N. Chatterjee and J. K. Mandal, "Detection of Blackhole Behaviour Using Triangular Encryption in NS2," 1st International Conference on Computational Intelligence: Modeling Techniques and Applications(CIMTA- 2013), vol. 10, pp. 524–529, 2013.

[11] A. Nadeem and M. P. Howarth, "A survey of manet intrusion detection and prevention approaches for network layer attacks," IEEE Commun. Surv. Tutorials, vol. 15, no. 4, pp. 1-19, 2013.

DOI 10.17148/IJARCCE.2016.56162