An Individual Trust Management Technique for Mitigating Sinkhole Attack in MANET

Khushboo Tunwal
M.Tech in Computer Science,
GWECA, Ajmer,
RTU, Kota

Priyanka Singh Dabi
M.Tech in Computer Science,
GWECA, Ajmer,
RTU, Kota

Pankaj Sharma
Assistant Professor,
GWECA, Ajmer,
RTU, Kota

ABSTRACT
MANET is considered as an infrastructure less data network where the nodes can behave as source or router (packet forwarder) which helps the network to cover the longer distances with low power transmission. Since it does not require any centralized controlling system and can organize itself without external interfere it's a preferable choice for the small battery operated clustered system such mobile and PDA. The self-organizing nature of MANET makes it very flexible and dynamic which can adopt variety of system configuration. Although to provide such services the protocols designed for MANET contains many security loop holes which makes it prone to network attacks and easy target for attackers. Although many types of active and passive attacks currently known, this paper focuses on Sink-hole attack which is a sub-category of Black-hole attack. The sink-hole is considered as one of the most serious attacks in MANET because it force the traffic to pass through attackers node by manipulating the routing protocol and then node drops all the traffic, which causes degradation of networks performance. This paper present an individual trust managing technique to prevent against sink-hole attack. The proposed algorithm is simulated using network simulator NS2 and the results shows that the proposed algorithm greatly reduces the sink-hole impact and performs much better than previous algorithm.

General Terms
Sinkhole attack, trust management technique.

Keywords
MANET, Sink-hole Attack, Black-hole attack, Individual Trust Management.

1. INTRODUCTION
The world is getting networked which facilities increased connectivity and lead to better communication and information sharing, to provide the reach of such interconnection at every place and for every application some specific type of networks are designed such as Zigbee, WSN and MANET. As it is already discussed the ad hoc network is a wireless network without any fixed infrastructure. A collection of mobile nodes called Mobile Ad Hoc Network (MANET) which behaves as routers also so doesn't required involvement of any coordinating infrastructure or centralized access point such as a base station. Besides providing such facilities it provides other challenges, including secure routing, QoS etc. since MANET does not use basic networking devices, such as routers or access points. Thus, data transfer among the network nodes is performed by the concept of multiple hops, and every node collaborates with the others for establishment and maintenance of routes rather than just behaving as a mobile host.

On the basics the MANET nodes within communicable radio range communicate directly by wireless links, while those that are not achievable by direct radio link uses other nodes as relays. In the overall communication process every node assumes that the other will behave according to the predefined rules hence a trust among them is always remains and this, help each other in conveying information throughout the topology of the network and share the responsibility of managing the network. The Sink-Hole attack exploit the multi-hop and quicker route establishment tendency of the MANET by which the nodes always try to communicate with the newest path. In Sink-Hole attack the attacker advertise itself as it knows the most recent route towards destination and when the source select the route through it then the node drops the packets hence degrades the network performance. This paper presents an algorithm to maintain trust as an indicator for their genuine behavior. The remaining paper is organized as follows: the second section provides a brief discussion of the most recent and relative literatures, followed by a basic review of MANET and the Sink-hole attack, in third and fourth section respectively. The fifth section explains the proposed algorithm and the simulated results are shown in the sixth section while the conclusion and future work on the basis of the simulation results is presented in seventh section.

2. LITERATURE REVIEW
Because of the critical personal and business information's are shared over the network the problem of security and cooperation enforcement has gain considerable attention by individual researchers as well as research organizations works on the ad hoc network community. In this section, some of these contributions are presented. Kisung Kim and Sehun Kim [2] proposed incremental learning algorithm for detection of sinkhole node on Dynamic Source Routing (DSR) protocol in MANET. Through analyzing the sinkhole detection problem they extract several sinkhole indicators. Edith C. H. Ngai et al [4] proposed algorithm in Wireless Sensor Networks for Detection for Sinkhole Attack. Their algorithm finds suspected nodes list, and then through a network flow graph identifies the adversary in the list. The algorithm is also good enough to deal with cooperative malicious nodes that tries to hide the real intruder. Et al [3] presented a useful review of different types of techniques used for Dealing with Sinkhole Attacks, such as Anomaly-based, Rule based, Statistical and Cryptographic they also discussed the literature published utilizing these approaches as basic idea. Ioannis Krontiris et al [5] discussed some of the techniques that an attacker can adopt to create sink-hole attack then propose specific detection rules that make legitimate nodes aware of the threat, while the attack is still taking place. Cryptographic Protocols to Fight Sinkhole Attacks is proposed by Anthonis Papadimitriou et al [6]. They introduces two new

cryptographic protocols with different computational complexity and decoding strength to limit network degradation on tree-based routing topologies in Wireless Sensor Networks (WSNs) caused by sinkhole attacks. The bot protocol is designed to provide continuous operation by improving resilience against, rather than detection of, these attacks. The benefit of providing resilience is that to induce the inherent ignorance property which allows operating in the presence of attacks. Furthermore, resilience mechanisms does not requires detection mechanisms but naturally ignores the attackers hence it reduces the complexity and the overhead required for detection mechanisms. Sinkhole Avoidance Routing is presented by Andrew J. Stephenson et al [7], under the Trident Research Project which is started to minimize the disruption from such an attack. They have proposed some changes on existing tree based routing protocol to make it immune to sinkholes attacks and increase the overall data throughput of the network. Although it compromises with networks transmission efficiency.

3. OVERVIEW OF AODV ROUTING IN MANET

AODV is presently the most widely used reactive routing protocol for a MANET. It establishes routes quickly over dynamic network connections, with small traffic overhead and low route storage memory consumption. Because it is reactive the nodes in the network deploys routing packets only when they want to communicate, and maintains the information updated only as long as the communication lasts.

When a node wants to send data (a packet) to another node a route discovery process is started by it in order to find a proper route to the destination node, this is done by broadcasting a route request message (RREQ) to its neighbors. Neighboring nodes who receives this message increment the hop count in the message on receiving the RREQ, and forward (broadcast) it to their neighbors. The process executes continually until the destination node for particular RREQ is found. The RREQ message forwarding used for other nodes to learn the reverse route to the source node. When the RREQ message reaches the destination node, a route reply message (RREP) is generated by the destination. The RREP is sent to the source node as a unicast along the reverse route which was established during the RREQ broadcast.

The intermediate node learns a forward route to the destination node after reading the RREP message similarly as they done during RREQ. Therefore, ones the route discovery process, found proper route packets can be delivered from the source to destination node or oppositely destination to source.

There are also route maintenance messages such as RERR: route error message used during the link breakage. HELLO: thus, every node knows which nodes are not its neighboring nodes within one-hop. All routing information expires after a timeout in case of an inactive route, and is removed from the routing table.

Being a collaborative protocol AODV allows nodes to exchange information about each other hence the RREQ messages do not necessarily required to reach the destination node during the route discovery process because an intermediate node having a route information to the destination can reply with RREP without any further broadcasting of the RREQ. This procedure helps in quicker route searching and eliminating unnecessary flooding of RREQs also.

Since the nodes in the network can be mobile hence the movement of nodes are possible hence after some time the stored routes may no longer useful hence to maintain the continuously Sequence numbers are used by AODV to identify fresher routing information. Sequence number is maintained by every node, and increments it before sending either a new RREQ or RREP message. The sequence numbers are recorded in routing tables and included in routing messages. AODV favors newer information, thus routing table is updated by the nodes whenever they receive a message with a higher sequence number (a larger number refers to newer information) or a smaller hop count (smaller hop count refers to shorter path) than what exists in the routing table for a given destination. However, a sequence number is given a higher priority than a hop count. That is, a route with newer information is favored even if it is longer. Being a reactive routing protocol, AODV doesn't give nodes a full view of network topology. That is, every node only knows its neighbors, but for the non-neighbors, it only knows the distance in hops and the next hop to reach them .

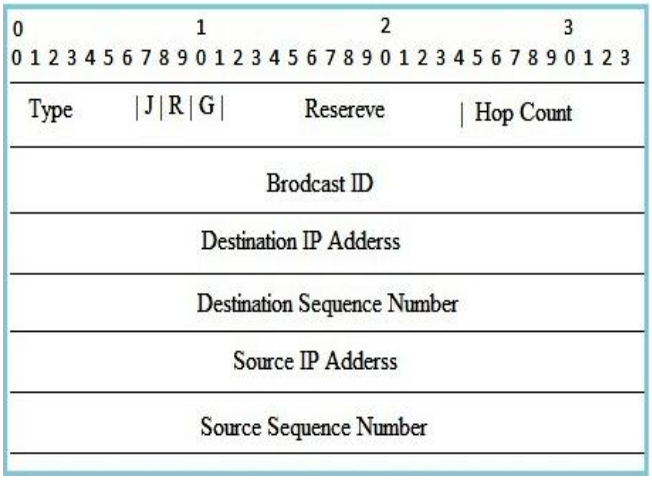

Fig 1: RREQ Packet Format for AODV

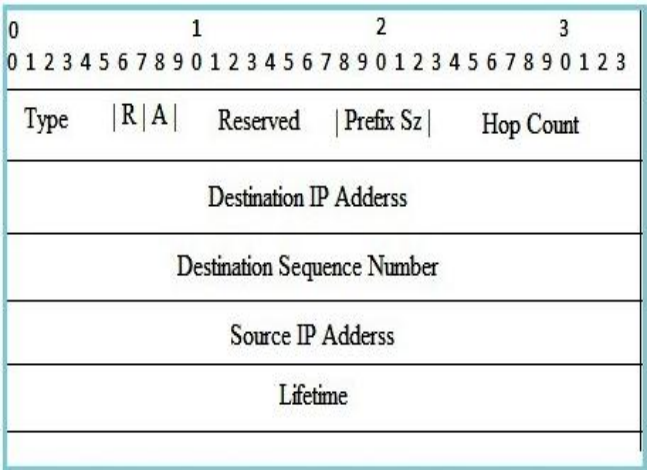

Fig 2: RREP Packet Format for AODV

However, the AODV's security is compromised by the Black Hole nodes, as the received RREP is accepted having fresher route. The threat of Black Hole attacks cannot be fought by the standard AODV routing protocol, because during the route discovery phase, a sequence number and hop count in the routing message may be counterfeited by malicious nodes;

thereby, the route is acquired, eavesdropping or/and as they pass dropping all the data packets.

4. SINKHOLE ATTACK

Sinkhole attack, a sinkhole node from all neighboring nodes tries to attract the data to itself. A fake routing information is generated that in local network lets the nodes know itself on the way to specific nodes. Sinkhole node attempts to draw all network traffic to itself through this procedure. Thereafter the data packet is altered or the packet is dropped silently. Sinkhole attack by boosting energy consumption decreases network's life time, increases network overhead, finally destroys the network [4]. In AODV protocol, by modifying sequence number sinkhole attack is set up in RREQ. Sequence number that is used to prevent loop formations indicates the recency of the route. The higher the sequence number, the more recent route the packet contains. The source, destination node is selected by the sinkhole node. It carefully observes the source node's sequence number and with selected source, higher sequence number and destination a bogus RREQ is generated. After adding itself on the source route, the bogus RREQ is broadcasted. Nodes that take this bogus RREQ recognize that a better route to the source could be reversed route than incumbent route.

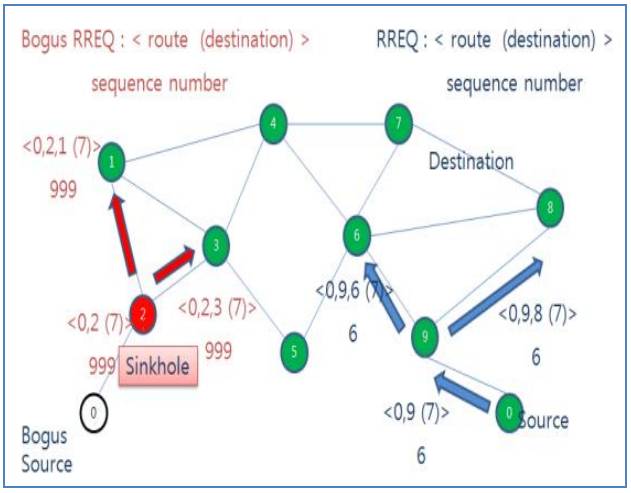

Fig 3:Generation of False RREQ by Sink-Hole Attacker

5. PROPOSED ALGORITHM

Because the sinkhole attack has the property to attract the network traffic and drop it. The proposed algorithm utilizes this behavior for detecting the avoiding the paths through such nodes.

Step 1: let the node S wants to send a packet to D, and an attacker A.

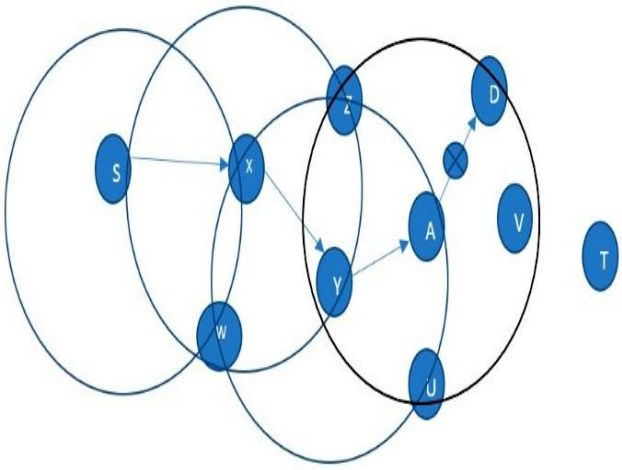

Fig 4: Demonstration of Proposed Algorithm.

Step 2: as shown in figure it's clear that even the source S is transmitting to D via "X,Y,A" the transmission of S to X can also be received as node W and the transmission of the X to Y is also received on W and Z.

Step 3: Now if the nodes are normally behaving they should forward the packets to next node until the destination reached, hence when the node W receives the transmission from S it waits for a certain time "Tm" to hear the retransmission from X also. If it doesn't it assumes that the node X is misbehaving and dropping the packets however this may not be true if the node moves out of the W's receiving range.

Step 4: hence every time the node assumes the node is malicious it decrements the local trust (LT) value for that node.

Step 5: now if node detects the transmission by a malicious node it resets the local trust (LT) for it.

Step 6: now when the route is created the nodes with the lowest trust values are avoided.

Step 7: to enhance the efficiency and reduce false alarming the time "Tm" is dynamically modified on the basis of the packets received per seconds. If the packets received per seconds are higher then there is a possibility of more forwarding delay hence the "Tm" is increased.

6. SIMULATION RESULTS

In order to evaluate proposed detecting method, we experiment with network simulator, NS2. The simulation set up for different percentage of Attacking Nodes and the simulation results are presented in graphical form.

No. of Nodes	Delivery Ratio			Delay Avg. (Seconds)			Jitter Avg. (Seconds)			Throughput (Avg.) Transfer (B/s)		
	Prop.	Pre.	Att.	Prop.	Pre.	Att.	Prop.	Pre.	Att.	Prop.	Pre.	Att.
5	0.8875	0.8436	0.818	137.16	157.06	153.2344	4.27	21.8	17.1	142	135	131
10	0.8812	0.8125	0.7787	156.86	157.63	169.9273	4.22	16.3	20.6	141	130	123
15	0.8375	0.7187	0.6937	121.54	173.49	162.6528	4.98	19.8	22.01	134	115	111
20	0.7937	0.6473	0.6375	152.33	180.93	169.9741	5.1	12.1	21.9	127	103	102
25	0.7312	0.6062	0.593	138.11	181.62	538.3482	4.8	19.6	19.12	117	97	95
30	0.7125	0.5375	0.506	186.13	187.26	535.2597	3.5	15.3	26.21	114	86	81

Table 4: Comparison Table between Proposed, Previous and Attack

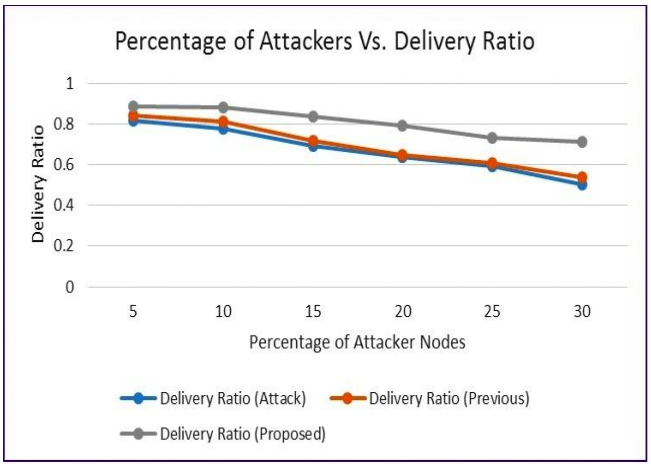

Fig 5: Comparison for Delivery Ratio for Different Percentage of Attackers.

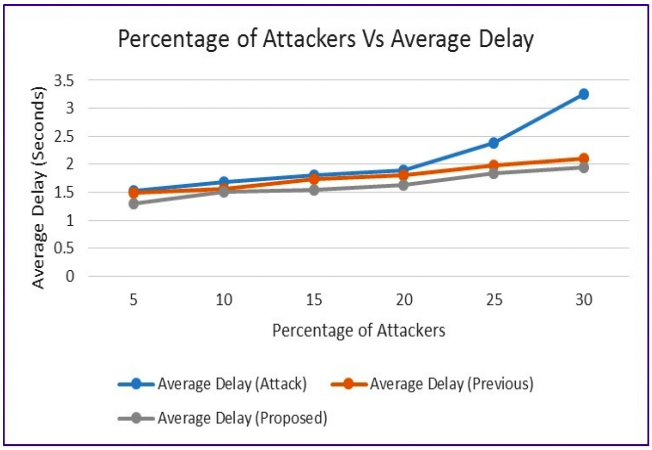

Fig 6: Comparison for Average Delay for Different Percentage of Attackers.

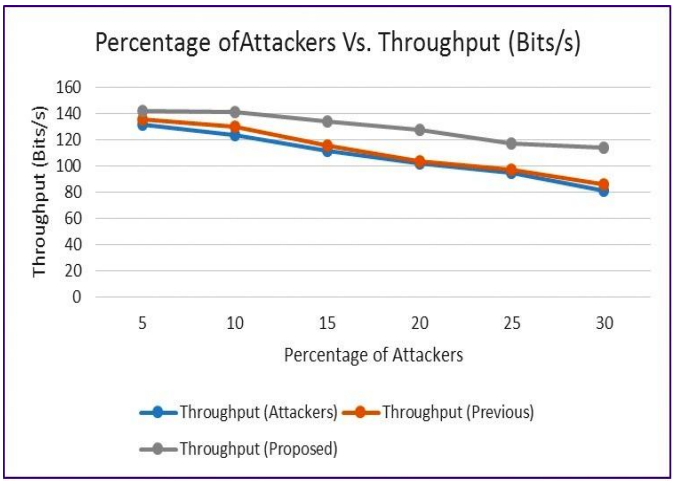

Fig 7: Comparison for Throughput for Different Percentage of Attackers.

7. CONCLUSION

In this paper, a sinkhole prevention method is proposed based on individual trust management algorithm. As an ad hoc network has a dynamic network topology, it is important to update the node reputation to immediately identify the malicious node. The proposed method can co-exist within a MANET with the changes and the sinkhole attack can be found precisely. The simulation, confirms that proposed method is well suited not only for high typical sinkhole attack but also for special version of sinkhole attack (stealthier attack or opportunistic attack) and robust to network environment. In future a dynamic threshold estimator may be designed to lower the false positive rate.

8. REFERENCES

[1] YANG XIAO, XUEMIN SHEN and DING-ZHU DU "Wireless Network Security", Signals and Communication Technology 2007, Springer.

[2] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in Proceedings of IEEE Consumer Communications and Networking Conference (CCNC '06), Las Vegas, USA, January 2006, pp. 640–644.

[3] Junaid Ahsenali Chaudhry, Usman Tariq, Mohammed Arif Amin, Robert G. Rittenhouse "Dealing with Sinkhole Attacks in Wireless Sensor Networks", Advanced Science and Technology Letters Vol.29 (SecTech 2013), pp.7-12.

[4] Jiangchuan Liu, Edith C. H. Ngai and Michael R. Lyu "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks", Communications, 2006. ICC '06. IEEE International Conference on (Volume:8) June 2006.

[5] Ioannis Krontiris, Thanassis Giannetsos, Tassos Dimitriou "Launching a Sinkhole Attack in Wireless Sensor Networks; the Intruder Side", Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing, 12-14 Oct. 2008.

[6] Fabrice Le Fessant, Anthonis Papadimitriou, Cigdem Sengul, Aline Carneiro Viana"Cryptographic Protocols to Fight Sinkhole Attacks on Tree-based Routing in Wireless Sensor Networks", Secure Network Protocols, 2009. NPSec 2009. 5th IEEE Workshop on 13-13 Oct. 2009.

[7] Andrew J. Stephenson, Dr. Eric Harder "Sinkhole Avoidance Routing in Wireless Sensor Networks", Trident Research Project Information Technology Major, May 9, 2011.

[8] Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy "Denial of Service Attacks in Wireless Networks: The Case of Jammers", IEEE Communications Surveys & Tutorials, Vol. 13, No. 2, Second Quarter 2011.

[9] Satyajayant Misra, Kabi Bhattarai and Guoliang Xue "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks", Communications (ICC), 2011 IEEE International Conference on 5-9 June 2011.

[10] Zahra moradi, Amir Masoud Rahmani, Mohammad Teshnehlab "Implimantaion of Neural Networks for Intrusion Detection in MANET", International Conference of Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on 23-24 March 2011.

[11] Junaid Ahsenali Chaudhry, Usman Tariq, Mohammed Arif Amin and Robert G. Rittenhouse "Sinkhole Vulnerabilities in Wireless Sensor Networks", International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.401-410.