ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 4.775, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

LIGHTWEIGHT TRUST SYSTEM TO RESIST RESOURCE DISSIPATION ATTACKS IN ADHOC WIRELESS SENSOR NETWORK

T. Edward Francis* & D. Arul Pon Daniel**
Department of Computer Science, Loyola College of Arts & Science, Mettala, Namakkal, Tamilnadu

Cite This Article: T. Edward Francis & D. Arul Pon Daniel, "Lightweight Trust System to Resist Resource Dissipation Attacks in ADHOC Wireless Sensor Network", International Journal of Computational Research and Development, Special Issue, January, Page Number 62-68, 2017.

Abstract:

Adhoc wireless sensor networks are limited resources, self organizing, and infrastructure less networks. These networks consist of deployed sensor nodes that sense and send information to the base station (BS) through the cooperative routing process. Due to this all the nodes are mandatory to forward packet for routing even message is unrelated to it. So, all the nodes act as a router to route the packet towards destination. This scenario can be utilized by the malicious node to cause the damage in the network. Vampire attacks are similar attacks that deplete the node's battery power by launching attack in the routing layer. These "vampire" attacks are instance of resource dissipation attacks which works over time to permanently disable the network. Such kinds of attacks are loop energy loss attack, carousel attack and stretch attack. Our proposed approach is lightweight trust scheme to prevent the network from resource dissipation attack. In this, Lightweight means to less energy to trust value calculation, trust value communication, attack detection and attack prevention. This paper proposes the lightweight trust scheme to prevent network from loop energy loss attack and intuitions to bound the damages caused by the carousel and stretch attack in the Lightweight trust scheme

Key Words: Resource Dissipation Attacks, Loop Energy Loss Attack, Power Draining Attacks, Routing Attacks & Trust Scheme

Introduction:

Ad hoc wireless sensor networks are power full combination of computing, communication and spatially distributed sensor nodes, which have limited battery power with it. In this century there are wide ranges of application domains in ad hoc wireless sensor network are health care systems [3], environmental monitoring[6], industrial machine monitoring[7], process monitoring, asset tracking, target tracking [4], home automation and many more in future. In this growing technology various issues and challenges are in research. Some of the core important research parts of ad hoc wireless sensor network are security and routing. Especially, routing is unavoidable to any network in the world. So there are very serious routing infrastructure attacks in ad hoc wireless sensor network which degrades the performance of the network and also lets to the resource dissipation. Dissipation of resources mentionable is CPU processing time, bandwidth of the network and battery power etc.., specially this resource dissipation attack can cause the higher degradation of network performance and resource wastage which may cause the less application performance and network survivability. Some of the familiar attacks like Denial of Service (DoS) attack [9], [13], [12], [11] Reduction of quality (RoQ), Routing Infrastructure attacks works over the time to completely deplete node's battery power is belongs to the instance of Resource dissipation attacks. There is another mentionable resource dissipation attack is Vampire attack. Vampire is complicated to define, which can be defined with help of the causes of the vampire. Very important cause of the vampire is to deplete the node's battery in the network and make entire network shut down. Usually in wireless ad hoc networks, packet transfer between source and sink is carried by the set of intermediate nodes between them. So a set of nodes will be involved in the transmission packets between source and sink, spends its energy for transmission of packet Even though it is irrelevant to it. All nodes are mandatory to involve in packet forwarding to the sink which can mention as cooperative process. So, here any adversary node can spent very minimal energy to construct the message and sent to the sink. The Energy spent for composing and sending message may be lesser that the cumulative energy spent for transmitting to sink. Considering this adversary node can sent same number of packets as like a honest node in the network to cause maximum damage to the network. So, vampire can be defined as a any malicious activity in the packet forwarding which cause more energy loss. Vampire which causes higher cumulative energy level which may let to entire network shut down by spending minimal energy on launching attack. Vampire spent very little CPU time to cause the huge cumulative energy loss in packet forwarding. Detection of vampire is quite hard in ad hoc wireless sensor network due to its adhoc organization and vampire's distinct characteristics from other attacks. Even vampire can cause very huge energy loss to the various minimal energy routing protocol because these protocols works with routing the packets with minimal energy which is not a limitation for the vampire. Vampire works over the time to entirely shut down the network even in minimal energy routing protocols. Contributions: This paper makes four contributions. First, to show the various kind of the vampire that causes the huge energy loss at the packet forwarding. Second we discuss the vampire in clustered adhoc wireless network. Third, we introduce lightweight trust system to resist vampire in the network and shows simulation results. Fourth, few intuitions to resist carousel and stretch attack, a kind of vampire (familiar directional antenna attack is considered). Overview: Vampire not only causes the energy drain to the node, but indirectly it affects the property of network survivability through the network partitioning. There are series of attacks that drains the energy are discussed with examples in this part. First attack we take for discussion is Loop Energy Loss Attack. Loop Energy Loss Attack can be defined as a same set of nodes take a loop to lose its energy. This can be considered as continuous sending and continuous dropping of messages. Where continuous sending by the source node to destination node, in that one of the malicious intermediate node continuously dropping packet as result packet never reaches the destination. But a set of nodes between source and malicious node, cooperatively involved in continuous transmission is energy draining process. Here malicious node spent very small CPU time to cause huge cumulative energy loss.

ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 4.775, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

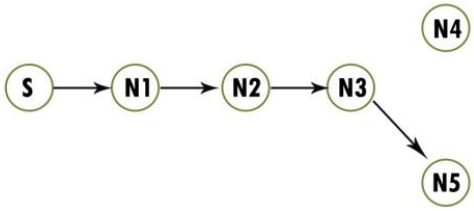

Figure 1: Loop Energy Loss Attack

Figure 1 show the example of Loop energy Loss attack, where source node S transmit the packet to destination node D. there N1,N2,N3,N5 are with the shortest distance intermediate nodes to reach destination node D. N5 is the malicious node which drops the packet with the intention to generate the loop energy loss attack. Due to the continuous sending by source and continuous dropping by the malicious node causes same set of intermediate node take a loop to drain its energy. Figure 2 shows the simulation graph for loop energy loss attack in NS2 [5]. The 19 nodes are considered for the simulation and loop energy loss attack is shown with different intermediate nodes. In loop energy loss attack as packet got dropped at the malicious node, the packet progression and cumulative energy loss is only between source and malicious node. So, the graph shows the cumulative energy loss between source and malicious node for different intermediate nodes, different no of packets. As intermediate node is increase, the cumulative energy loss also increases is show in the graph. Energy loss is considered for different no of packets transmission like 1packet (mentioned in red line), 10packets (mentioned in green line), 100packets (mentioned in blue) and 1000packets (mentioned in pink) with different no of intermediate nodes.

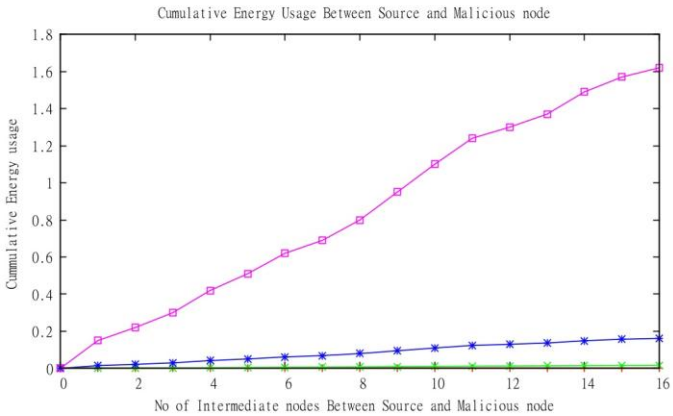

Figure 2: Energy Loss due to Loop energy loss attack for 1packet, 10 packets, 100packets, 1000 packets

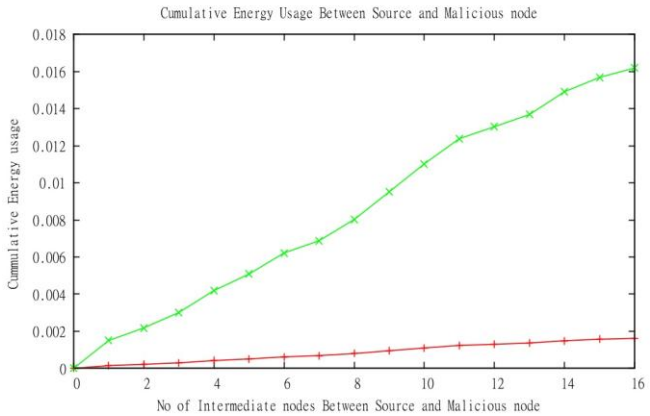

Figure 3: Zoomed view for 1packet and 10packets transmission

Figure 3 shows the zoomed view of 1packet and 10packet transmission cumulative transmission energy loss with different no of intermediate nodes. This shows the more no of packets with more no of intermediate node will cause huge cumulative energy loss. The second attack we discuss is Carousel Attack [14]. Carousel can be defined as transmission of same packet within the set of nodes for infinite no of times by adversary. Adversary node causes its damage by creating loops among the nodes to drain its battery level called carousel attack. Generally carousel attack not only drains the battery level of the nodes involved in transmitting but also never delivers the packet to the sink. This put packet delivery unreliable. If more packets is looped within a set of nodes this results in increased network traffic that lets bandwidth exhaustion. Figure 4 shows that the diversion of packet from N5 to N3 instead of sending to D with the intention to form a loop by the malicious packet. So set of nodes involved in the transmission of malicious packet within the loop will waste its energy in transmission.

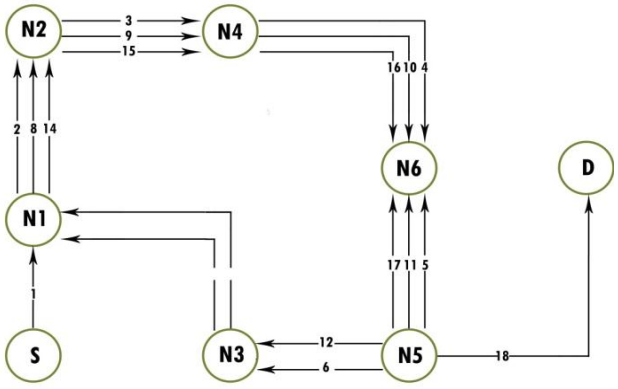

Figure 4: Carousel Attack

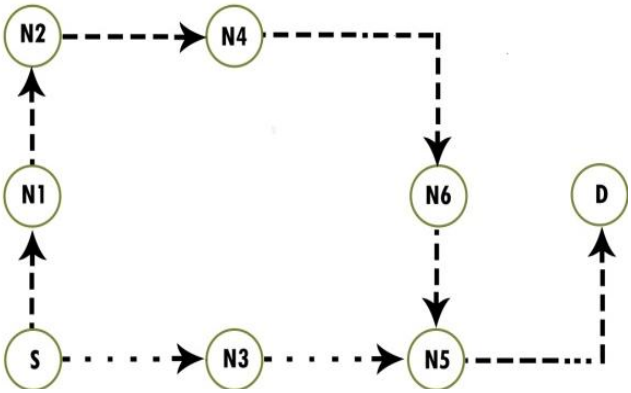

Figure 5: Stretch Attack

Our third attack that drains energy is stretch attack [14]. In Stretch attack adversary node constructs the artificially longest route so that packet traverses the longest path to reach the sink. When packet travels to the longest path with more number

ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 4.775, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

of intermediate nodes will also causes unwanted loss of energy due to the longest path and more intermediate node involve in transmission. Stretch attack also increases the packet delivery time that lets to performance degradation for sensing applications. Figure 5 shows the stretch attack, where shortest path is mentioned with the dotted lines and malicious route are mentioned as dashed lines. Stretch attack that aims at increasing the path length. So that the packet should be transmitted by the more no of intermediate nodes in compare to genuine path (genuine path are shortest path to reach destination). Figure shows the genuine path in dotted lines with two intermediate node to reach destination and dashed line with malicious path consist of five intermediate nodes to reach same destination. Malicious path consist of more no of intermediate nodes so cumulative energy required for the transmission is also higher than the genuine path. The worst case of the stretch attack is when the packet reached all the nodes in densely deployed adhoc wireless sensor network to reach its destination even there are genuine node. Maximum damage can cause by the stretch attack is depending on the size of the network. For the better understanding figure 6 shows the honest scenario, in that source node1 sends the packet to the destination node 6through the shortest genuine path, the packet transmission is mentioned with arrow mark. The figure 7 shows the stretch attack for the same scenario. The packet transmitted by the node1 travelled through the longest path to reach destination is show with arrow mark. In the same figure carousel also mentioned between set of nodes (node9, node18, node10, node13, node15). The packet send by the node12 has to reach destination node16 instead packet took its way to node 15 and forms the circular path.

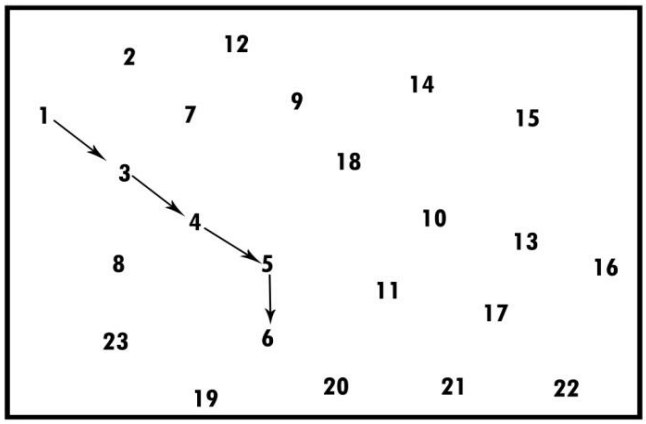

Figure 6: Honest Scenario

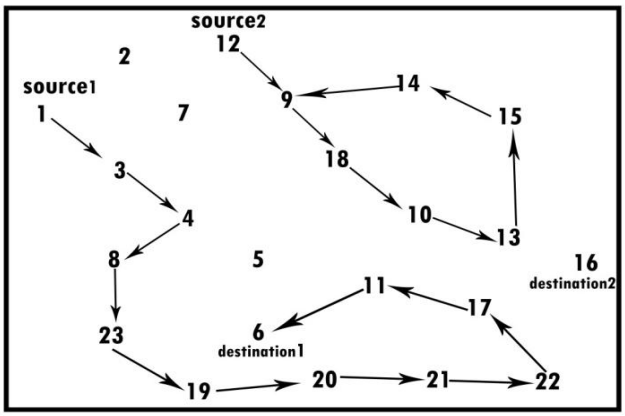

Figure 7: Stretch and Carousel Scenario

Generally these attack can be bounded by defining packet time to live (TTL) according to the diameter of the network. If the no of nodes n the network is pre known then graph – theoretic technique can be used to calculate the diameter of the network. Still intelligent adversary can change the path length and TTL to the higher values to cause damage. But it is unformulated how to discover and secure to work with TTL values. To calculate the network diameter there few algorithms that can be accurate even in adversary presence [21] [17]. Those algorithms also need few works to be formulated to make it suitable for various scenarios.

Related Work:

In this paper we propose lightweight trust system to resist the vampire attack in adhoc wireless sensor network. There are various work related to the energy draining attacks. Such attack is denial of sleep attack [25] which considered in the MAC layer but our adversary works on the routing layers of various protocols to launch attack. J.-H. Chang et al. proposed the energy efficient routing algorithm for the transmission of packets. Main objective of maximum lifetime routing in wireless sensor network [29] paper is to maximize the network lifetime. And also paper emphasis that power consumption is closely coupled with route selection. Even though paper deals with maximization of network lifetime by means of routing our adversary is long term attack that can work over long time to disable entire network. Yih-chun hu et al. proposed the protocol called Ariadne [22]. The goal of the paper is to prevent the denial of service attack (DOS) and prevent the uncompromised route. Ariadne protects against the adversary causing the invalid network path but vampire uses the valid network path for attack. Y.-C. Hu et al. discusses about detection of wormhole attack [15], a serious and challenging attack even possible in all the communication that follows authenticity and confidentiality. Wormhole attack is also possible without compromise any host. This attack tunnels from one location to another location. Wormhole can influence the attacks like DOS, disrupt routing, and gain unauthorized access. This paper proposes detection of wormhole using the packet leashes. They are categorized to two types of leashes geographic leashes and temporal leashes. Geographical leashes are constructed by using the nodes own location and loosely synchronized clock. While sending the packets, sender adds its own position Ps and sending time Ts to the packet. At the time of receiving, receiver compares value with its own position. Considering temporal leashes, messages are added with the time Ts at sending, in the receiver side receiving time is compared with the received packet where all the nodes are tightly synchronize. But these are the costly method will not me suitable for a lightweight system. M.G. Zapata et al. discuss an overview of security architecture for mobile ad hoc networks (SAM)[8]. The goal of SAM is to ensure the exclusion of selfish nodes, node authentication, and pseudonyms and secure routing. The secure routing protocol prevents against ignoring route request, directing the packet to longest non optimal path and invalid network path or route disrupt. But vampire does not cause invalid path, disrupt route or alter discovered path. Instead it uses the valid network path for the attack to cause the energy drain. R.C. Shah et al. proposed a paper on energy aware routing for low energy ad hoc sensor networks [30] which aims at the important metric called network survivability which is very use full metric for routing protocol performance. And also author suggest that always choosing lowest

energy path for routing will not be suitable for long term connectivity and network lifetime. Author proposed new energy aware routing which uses sub optimal path occasionally to obtain substantial gains. Our Adversary can still increases the energy even in Energy aware scenario because of long term availability. The protocol called clean – slate sensor Network routing [10] is also known as PLGP. This protocol is designed for secure communication even in presence of adversary in the wireless sensor network, which is so efficient and highly resilience to the active attacks. Even PLGP is secure protocol for ad hoc wireless sensor network, is still vampire presence will cause huge loss to energy. Author considered the familiar directional antenna attack which takes packet from one part of the network to other part of the network. So the node receive the packet will not know, from whom the packet is received. Receiving node has only known the packet and its destination network address. So receiving node cannot assure that packet it received is travelled and travel closer to the destination. But receiving legitimate node has only provision of taking the packet further closer to the destination. If the packet reached the other corner of network by the adversary, packet has to traverse long distance to reach its original location, which is the sink. This may cause cumulative energy loss and nodes involved in transmission. Assume that again the same packet comes to the same adversary. If this happen again and again this may be the worst case can causes the carousel attack which may result in huge energy loss to the set of nodes or all the nodes in the network who involved in packet forwarding. In the existing PLGP forwarding phase is modified to resist vampire The modified version of the PLGP is PLGPa [14], which is abbreviated as PLGP with attestation. . Every packet traverse in the PLGPa network is chain attested by the forwarding node in network. With that every node receiving can verify that packet is closely progressed towards the destination or not. Even in malicious or non malicious environment all the nodes process the packet should attest and verify. This is a heavy weighted process. If the environment is non malicious then, this attestation and verification itself an energy draining process

Analysis of Vampire Presence in Clustered Network:

Aim of the vampire is to devastate the energy of the node to shut down and reduce the network life time. Still the vampire is less effective to make damages in cluster adhoc wireless network architectures due to clustered routing and Trust managements. There is various clustered based architecture [28] available for adhoc networks. Clusters are nothing but virtual groups. In other words nodes in network are partitioned to many small groups called clusters. Each cluster have a leader to perform network related operation like routing, trust management..etc., this leader is called as cluster head. Cluster heads are elected with various election algorithms. Generally the cluster election algorithm uses the parameter like computing power, memory, and energy level of the node to choose as a good cluster head. Members with in the cluster are called cluster members. Cluster act as a gateway for the all the operation within the cluster. Communication among the nodes considered to be Inter cluster communication and intra cluster communication. Important benefits of using clustered architecture are limited energy, Network life time, resource efficiency, limited abilities, and application dependency. In the clustered architecture vampire cannot cause more damage. Assume that there are 100 nodes in the network with 10 clusters and cluster head. So, route discovery, route maintenance and packet forwarding are handled by the clustered head where all the communications are limited to the cluster heads as a first level so vampire is limited to cause the damage due the organization of clustered architecture.

Lightweight Trust Scheme to Resist Vampire:

Trust schemes are multifunctional control mechanism that establishes connectivity with the trusted nodes in neighbors and also helps to find the trusted routing path for reliable communication. Every node in the network has to calculate the trust values by observation of the neighbors when they do communication with it. There are two familiar known methods to find the trust value of the node. One is through the direct method. In direct method every node directly calculates the trust values of its neighbors by referring to the history of successful and unsuccessful interactions. Another method is indirect method, in that remote feedback about the node is collected from its neighbor nodes or other nodes in the network. As adhoc routing is a collaborative scheme, trust mechanism can help routing protocol to do the reliable packet transfer in the hostile environment. Basic idea of the trust system is to decide what to do from the history of activities and its results. Very important part of the trust system is trust estimation. If the trust estimation scheme is worthless in identifying misbehaving and malicious node that will highly degrades the performance. So trust estimation plays important role to find trusted and entrusted nodes in the open and hostile environment of adhoc wireless sensor network. Trust system supports the adhoc wireless sensor with assisting routing, security and control. Considering the densely deployed sensor nodes in the large scale environment, every node in the network is employed for sensing the information of its region which is the primary motive of deployment. Addition to it, all the node should work for routing, route maintenance and secure against the routing attack. So to make efficient and ease of operation clustered are employed in adhoc wireless sensor network. Clustering is grouping the set of nodes which are governed by clustered head for all the activities like routing, route management...Etc, the entire node in the cluster will send the sensed sensitive data to the clustered head. Cluster head takes the in charge to aggregate the data of clustered region and routing it to the base station [24]. The security concern, instead of making all the nodes with the heavily weighted code to secure against the attacker it is highly efficient to employ clustered head to work towards security. If the cluster formation and reliable cluster head election algorithms are efficient and lightweight, then the performance will be good. Clustering can also improve the throughput and scalability of the network [18]. Bringing the trust mechanism to the clustered architecture will add many more benefit for secure adhoc wireless network design. Cluster head can be assigned to find the faulty, misbehaving malicious node within the cluster. Indirect method of estimating the global trust value will become easy by using the cluster head. Cluster is also responsible for trusted route establishment to reach the base station. As our adversary targets the draining energy and nodes are limited with resources. The system we design to resist vampire like attack should be lightweight and energy efficient system. We choose LDTS – lightweight and dependable trust system [20] for clustered wireless sensor network to resist vampire like resource dissipation attack in the

ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 4.775, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

network. In the various trust schemes indirect method is done through broadcasting feedback messages to the other nodes. Broadcasting for the remote feedback collection will not be a efficient scheme. In the paper [20], all the nodes in cluster will sent the remote feedback about the neighbors periodically to the cluster head (CH). Whenever cluster members (CM) need feedback about the particular node it doesn`t need to broadcast instead it should sent one request to the CH. Cluster head will reply to the requested node with the trust value. Some trust scheme fails to make dependability as adhoc wireless sensor network is open and hostile environment. There is the possibility of getting wrong or malicious feedback from the malicious node. So the dependability of the system is ensured in this scheme with Global Trust Degree (GTD) evaluated with help of the aggregated remote feedback collected from all the nodes. This scheme uses the less memory overhead and less transmission overhead while handling trust values. Less over head in communication influences the less transmission power will be required for transmission of trust values.

We propose MLDTS as a lightweight trust scheme to resist loop energy loss attack which is the instance of resource dissipation attack. MLDTS is Modified LDTS for clustered adhoc wireless network. We use AODV protocol for routing purpose [1],[2]. Nodes in the network are grouped as clusters using the clustering scheme [16] and [19]. The integrity of the trust values transmitted between the nodes through the communication channel are ensured using key management schemes [22],[26], [27]. Otherwise intelligent malicious node can modifies thee the trust values when they are at transmission in the channel. AODV [1] is one of the on demand routing protocol and well flexible for dynamic self starting networks. Once the cluster formation and cluster head election is over, nodes in the network are ready to communicate. Whenever node interact with the another neighbor node in the network, the node transmitting the packet should observe that node is receiving the packet or not and it forwarding to the next node or not by using the promiscuous mode. The trust value can be mention between 0 and 10, so that they need very less memory (0.5 byte – 4bits) to store and less energy to transmit. If the nodes Ni transmit the packet to node Nj then node Ni will observe and increment the value of the successful interaction if successful. Or else Nj is not transmitted in the mentioned threshold then Ni record the unsuccessful interaction minus one for the node Nj. From the values of successful and unsuccessful interaction trust values can be calculated by using the following formula for CM – CM, CH – CH trust calculation

$$\mathcal{T}_{x,y}(\Delta t) = \left\lceil \left(\frac{10 \times s_{x,y}(\Delta t)}{s_{x,y}(\Delta t) + u_{x,y}(\Delta t)} \right) \left(\frac{1}{\sqrt{u_{x,y}(\Delta t)}} \right) \right\rceil$$

Where $\lceil \cdot \rceil$ is the nearest integer function, $\mathcal{T}_{x,y}(\Delta t)$ is the trust value of node x for y. Δt is the window time, it is used to mention the time till the trust values are valid. After to the mentioned time history of experience will be discarded and system will start to record the new experience and trust values. $s_{x,y}(\Delta t)$ is the successful interaction of node x with the node y. $u_{x,y}(\Delta t)$ is the unsuccessful interaction of node x with the node y. in the formula

$$1/\sqrt{u_{x,y}(\Delta t)}$$

is used to punish the node by reducing the trust values to the node to those suddenly changes its behavior to be malicious. For example if node x has 10 successful interactions and 1 unsuccessful interaction then the trust value is 9. In other case, node x has the 10 successful interaction and 2 unsuccessful interactions with the trust value of 6. Every node maintains the trust value in the matrix form. Cluster head also do the same to maintain the trust values when it interacts with other Cluster heads. But cluster members will periodically send the trust values of the other nodes to the cluster head. In CH – CM trust calculation Cluster head aggregate and calculate the GTD of the CM using the formula

$$\mathcal{R}_{ch,y}(\Delta t) = \lceil 10 \times E(\varphi(p|r,v)) \rceil$$

Where $\lceil \cdot \rceil$ is the nearest integer function. Posteriori probabilities of binary events are mentioned with p. r is the positive feedback of the y taken to the account when the trust value is greater than 5. V is the negative feedback counted to the account when trust value is lesser than 5 from the cluster members about y. so the probability expectation value for the beta distribution of p,r,v is given in the following formula

$$E(\varphi(p|r,v)) = \frac{r+1}{r+v+2}.$$

By using the same method BS – CH GDT trust for cluster heads are calculated. From the discussed formulas we can clear understand that calculation of trust value by CM, CH and BS are simpler and efficient. Whenever the packets dropped or failed to forward by the node are identified by the sender's observation. Then the sender will increment the unsuccessful interaction counter as a result, trust value of the node will become low. If the trust value is poor then node will not be considered as a trusted node and packet will be diverted to the alternate node that has a higher trust value. Through MLDTS we can avoid the Loop Energy loss attack that drains energy. Figure 8 shows the graph for packet delivery ratio at different time, with three malicious nodes which launches the Loop energy loss attack in the network. In the initial stages of communication PDR is decreased because of the malicious node but our proposed system has improved the PDR by finding the trusted node and trusted route to route the packet. After the few communications malicious node will have the poor trust value and they will be discarded by the other genuine nodes for packet forwarding. This discarding will make the good connectivity with the trusted nodes will results in stable and higher PDR in the network.

ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 4.775, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

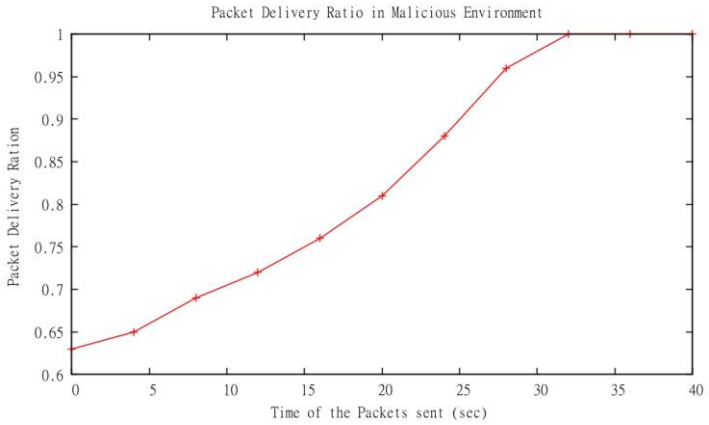

Figure 8: Packet Delivery Ratio

MLDTS is suitable to resist most of the energy draining attacks like carousel and stretch attack. In the paper [14] author justifies stretch and carousel using the familiar directional antenna attack. In that, this directional antenna take the packet at one location of the network and deposit to another part of the network that is not related to the path to reach destination. Now the packet has to travel long distance to reach the destination, this is considered as a stretch attack. If the same packet again and again comes to the adversary and adversary throws the packet again and again to the other part of network is the carousel attack. We discuss the intuitions in MLDTS to resist the carousel and stretch due to the directional antenna attack. Any node sending the packet or forwarding the packet should digital signature the packet with its identity. Any node receiving the packet should verify and identify the sender and lookup whether sender is the neighbor or not using routing table. If it is not a neighbor then the packet is diverted or sends by the adversary. Any packet can be received only from the neighbors who are within the coverage. So, node signed in the packet is not a neighbor of the receiver then the packet is forwarded by the adversary. So by dropping the malicious packet we can avoid energy draining in the network. There are many solutions for resource dissipation attacks in routing layer, making modification to the routing layer to resist resource dissipation attacks will make the routing algorithm complicated and these solutions will be energy draining process in non malicious environment. There are three parameter of the network to assure the performance of the network. They are shortest reliable route, less energy to transmit and less delay to reach destination. If these are good in the network we can say network operations are not intervened by the malicious node, because malicious nodes only reduce the performance of these parameters to degrade the performance. Our adversary with the intention to reduce the energy of the nodes in the network so at some point of time complete network will shut down due to individual node energy draining by the attack. Other two parameters are indirect aim of our adversary to cause damage. As our adversary is the long term availability. They are difficult to bound the damages caused. So, our proposed lightweight trust scheme can resist these types of resource dissipation attack efficiently.

Conclusion:

In this work, we proposed a Modified LDTS for clusterd adhoc wireless sensor network to efficiently detect and prevent network from vampire attacks which aims at draining the enrgy of the nodes. Proposed scheme is not only efficient but it is energy saving scheme to deal with the limited resource network. The goal of the vampire to devaste the energy, in contrast proposed scheme saves the energy for trust value estimation and trust feedback communication. Addition to that, clustered architecture also limits the damages caused by the vampire. we proposed scheme to resist the loop energy loss attack in the network which is the instance of resource dissipation attack. More to that, some intuitions are given to bound thecauses of carousel and stretch attack. In the cooperative environment like adhoc network, need the trust scheme to prevent the network from malicious activity. Our proposed scheme needs less memory to store trust values and less communication over head in remote feedback collection compared to the other trust schemes. Our proposed system is lightweight by means of calculation, communication, detection and prevention of resource dissipation attacks. As a future work intuitions given in the paper can be stimulated to analysis the performance in the malicious environment. And also energy draining attack in route and topology discovery phases are left for the future work.

References:

1. Charles E. Perkins and Elizabeth M. Royer. "Ad hoc On-Demand Distance Vector Routing." Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100.
2. Chakeres, I.D., Belding-Royer, E.M."AODV routing protocol implementation design ", Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on March 2004, pp 698 – 703.
3. Krco, S. “Health Care Sensor Networks—Architecture and Protocols,” Ad Hoc. Sensor Wireless Networks 2005, 1, 1–25.
4. Yang, H.; Sikdar, B. A Protocol for Tracking Mobile Targets Using Sensor Networks. In Proceedings of SNPA'03, Anchorage, AK, USA, May 2003; pp. 71–81.
5. “The Network Simulator - ns-2,” http://www.isi.edu/nsnam/ns, 2012.
6. Luís M. L. Oliveira , Joel J. P. C. Rodrigues “Wireless Sensor Networks: a Survey on Environmental Monitoring,” Journal of Communications, Vol. 6, No. 2, April 2011, pp. 143 -151.

7. Xingfa Shen., Zhi Wang,Youxian Sun., "Wireless sensor networks for industrial applications", Intelligent Control and Automation, 2004. WCICA 2004. Fifth World Congress on (Volume:4), June 2004, pp 3636 – 3640.
8. M.G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. First ACM Workshop Wireless Security (WiSE), 2002
9. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.
10. B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM
11. CoNEXT Conf., 2006.
12. J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.
13. A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.
14. J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.
15. Eugene Y. Vasserman and Nicholas Hopp "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" IEEE Transactions on Mobile Computing, Vol. 12, No. 2, February 2013,pp 318 – 332.
16. Y.-C. Hu, D.B. Johnson, and A. Perrig, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc IEEE INFOCOM, 2003
17. W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application- specific protocol architecture for wireless microsensor networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670, Oct. 2002.
18. A. Kro¨ ller, S.P. Fekete, D. Pfisterer, and S. Fischer, "Deterministic Boundary Recognition and Topology Extraction for Large Sensor Networks," Proc. Ann. ACM-SIAM Symp. Discrete Algorithms, 2006.
19. D. Kumar, T. C. Aseri, and R. B. Patel, "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks," Comput. Commun., vol. 32, no. 4, pp. 662–667, Apr. 2009.
20. O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for Ad-Hoc sensor networks," IEEE
21. Trans. Mobile Comput., vol. 3, no. 4, pp. 366–379, Oct. 2004.
22. Xiaoyong Li, Feng Zhou, and Junping Du "LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks" IEEE Transactions on Information Forensics And Security, Vol. 8, No. 6, June 2013.
23. Y. Wang, J. Gao, and J.S.B. Mitchell, "Boundary Recognition in Sensor Networks by Topological Methods," Proc. ACM MobiCom, 2006.
24. Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002.
25. A. Perrig, R. Szewczyk, J. D. Tygar, V.Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," Wireless. Netw., vol. 8, no. 5, pp. 521–534, May 2002.
26. R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee, "Group-based trust management scheme for clustered wireless sensor
27. networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp. 1698–1712, Nov. 2009.
28. D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network
29. MAC Protocols," IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009.
30. S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in Proc. 10th ACM Conf. Computer and Comm. Security (CCS'03), 2003, pp. 62–72.
31. C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in Proc. Second Int. Conf. Embedded Networked Sensor Systems (SenSys'04), Nov. 2004, pp. 162–175.
32. Yu, J.Y.; Chong, P.H.J. A Survey of Clustering Schemes for Mobile Ad Hoc Networks. IEEE Commun. Surv. Tutorials 2005, 7, 32– 48.
33. J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.
34. R.C. Shah and J.M. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks," Proc. IEEE Wireless Comm. And Network Conf. (WCNC), 2002.