International Journal on Applications in Engineering and Technology
Volume 2: Issue 1: January 2016, pp 4-8 www.aetsjournal.com ISSN (Online) : 2455-0523

ENHANCED COLLABORATIVE CONTACT BASED APPROACH FOR DETECTING SELFISH NODES IN WIRELESS NETWORKS

Deepica.K, Keerthana.S, Shifa Parveen.S, Silpa Das.K.S, - Guided by Mrs.Beaulah David

Abstract
The growth of mobile devices led to the wide use of mobile Ad-hoc networks(MANETS).It is necessary to detect selfish nodes so as to improve the efficiency of the network.Node misbehaviour due to selfish or malicious reasons can significantly degrade the performance of mobile Ad-hoc networks.The use of watchdogs is a well known mechanism to detect selfish nodes.It leads to poor network performance in terms of precision and speed.We propose a Reputed Information Exchange(RIX) scheme that reduces the packet transmission time and increases the precision.we implement the selfishness attack and analyze its effect on the packet delivery ratio, packet drop, overhead and packet delay.An Elliptic Curve Digital Signature Algorithm is used to detect and overcome the activity of selfish nodes.

Keywords: MANETs, Watch Dog, ECDS Algorithm, Selfish Nodes Detection, Network Performance.

1. Introduction

Ad-Hoc networks have no infrastructure where the nodes are free to join and left the network. The nodes are connected with each other through a wireless link. A node can serve as a router to forward the data to the neighbour nodes. In this model,the node misbehaviour is detected in the form of fully selfish and partially selfish nodes.The watchdog method fails to satisfy the efficiency and performance of the network.In order to enhance the detection rate and performance, an Reputational Information Exchange approach is used.It acts as a powerful tool for the detection of selfish or malicious nodes without centralised administration.The main objective of this work is to design an Elliptic Curve Digital Signature Algorithm taking into account attacker strategies and detection of malicious nodes in the delay-tolerant networks.

2. Related Works

For countering selfish attacks, a number of techniques have been reported in recent times. In [1]“Self-Policing Mobile Ad-hoc Networks by Reputation Systems” by Sonia Buchegger ,J.Y.Lebondde deals with node behaviour due to selfish or malicious reasons or faulty nodes significantly degrading the performance of mobile adhoc networks.To cope with misbehaviour in such self organised networks ,nodes need to be able to automatically adapt their strategy to changing levels of cooperation. The Reputation system in all nodes makes them detect misbehaviour locally by observation and makind use of second hand information. In [2]”Light Weight Sybil Attacks in Manets”proposed an RSS-based detection mechanism to safeguard the network against Sybil attacks.It can detect both join-and-leave and simultaneous Sybil attackers with a high degree of accuracy. In [3]”Crossing over the bounded domain – from exponential to power law intermeeting time in manets” by H.Cai,D.Y.Eun uses the Random Walk Model which provides guidelines on mobility modeling, performance analysis, and protocol design to survive the “curse” of the power-law distribution of the intermeeting time in MANET that Helps to identify nodes mobility. We can understand the performance tradeoffs in MANET obtained under the exponential distribution of the intermeeting time. In [4]”Impact of human mobility on opportunistic forwarding algorithm”by P.Hui, C.Diot,A.Chaintrean,,J.Crowcroft, proposed anInter contact time distribution algorithm is used to identify the exact packet delays .Analyzed several network scenarios for opportunistic data transfer among mobile devices carried by humans using eight experimental data sets. In [5]”Improving selfish node detection in manets using a collaborative watchdog” by A.Suhil kumar,Devanproposed a collaborative watchdog based on contact dissemination of the detected selfish nodes. Introduced an analytical model to evaluate the detection time and the cost of this collaborative approach. Reduce the overall detection time with a reduced overhead.In [6]”Trust and cluster based security in manets” by S.Sivagurunathan,K.Prathap chandran proposed a cluster formation and trust management approach which identify the packet delays and maintain the communication overhead over all the network. In [7]”Comparative study of techonology used for detection of selfish nodes” proposed an auction based AODV routing mechanism where the selfish nodes can be detected and partial selfishness can be found but no remedial actions is taken. Deletion is possible but replica allocation can’t be implemented.

3. Existing system

In the existing system, CoCoWa as a collaborative contact-based watchdog to reduce the time and improve the effectiveness of detecting selfish nodes, reducing the harmful effect of false positives, false negatives and malicious nodes.

CoCoWa is based on the diffusion of the known positive and negative detections.

When a contact occurs between two collaborative nodes, the diffusion module transmits and processes the positive (and negative) detections.CoCoWa can reduce the overall detection time with respect to the original detection time when no collaboration scheme is used, with a reduced overhead (message cost).Finally, using CoCoWa we can reduce the effect of malicious or collusive nodes. If malicious nodes spread false negatives or false positives in the network CoCoWa is able to reduce the effect of these malicious nodes quickly and effectively.

CoCoWa is also effective in opportunistic networks and DTNs, where contacts are sporadic and have short durations, and where the effectiveness of using only local watchdogs can be very limited.

Disadvantages:

1. Time consumption and efficiency increases
2. Effectiveness of Watch dogs is limited.
3. Increases the communication overhead

4. Proposed system

The proposed technique used to combat node misbehavior in network using reputation-based. In such schemes, network nodes collectively detect and declare the misbehavior of a suspicious node. Such a declaration is then propagated throughout the network so that the misbehaving node will be cut off from the rest of the network. And the selfish nodes will be punished and good nodes will be prioritized along with credit point.The proposed system overcomes the above drawback of watchdog by implementing a new method which is the combination of Reputation based schemes. Data anonymization techniques help to prevent from partial selfishness attackers.

Based on the reputation score and positive score selfish node will be identified and punished according to their reputation score, and the best node will be elected as a CH.

Reputation based scheduling scheme enables the client node to send data with priority.

4.1Modules:

List of modules:

1. Network module
2. ECDSA/RIX
3. Simulation results
4. Performance analysis

Network modules

1. The implementation is generating mobile nodes.
2. Number of mobile nodes will be initiated in the topography.
3. The node properties such are node id, initial bandwidth and RREQ, RREP etc.,
4. It utilizes the C++language

RIX Modules:

1. The configuration module has two faces

   - initial setup
   - user registration.
2. During the initial setup phase, the RIX generates a key (public/private key pair). Example e-mail user id (public key),password(private key)
3. Anonymous Key generation and authentication:
4. random key generation algorithm is used in this model
5. Additionally the key verification and authentication is required to ensure that services are offered to nearby entities.

Reputation modules

1. Malicious activities of the node has been identified.
2. Node behaviour such as holding node for longtime, sending false positive and negative nodes.
3. According to the node behaviour :

   -Detection
   -Replacement
   -Analysis of shortest paths are identified.

Simulation results

1. The final output in Network animator window.
2. Trace file contains topology information, Example - nodes, links, as well as packet traces.

Performance Analysis

1. The performance of this routing protocol and evaluated the performance
2. The performance analysis is based on packet drop ratio, overhead, packet delay and delivery ratio.

Advantages

1. The proposed system overcomes the above drawback of watchdog by implementing a new method which is the combination of Reputation based schemes. Data anonymization techniques help to prevent from partial selfishness attackers.
2. Based on the reputation score and positive score selfish node will be identified and punished according to their reputation score, and the best node will be elected as a CH.
3. Reputation based scheduling scheme enables the client node to send data with priority.

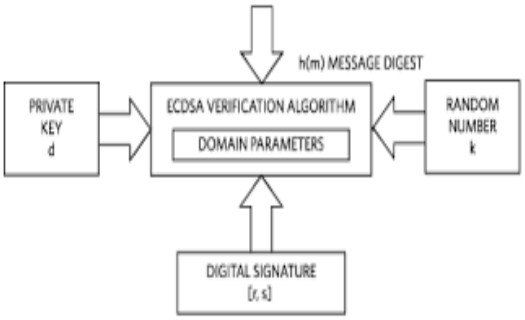
4.1 Elliptical Curve Digital Signature Algorithm

1. Calculate $e = \mathrm{HASH}(m)$, where HASH is a cryptographic hash function, such as SHA-2.
2. Let z be the L_n leftmost bits of e, where L_n is the bit length of the group order n.
3. Select a **cryptographically secure random** integer k from $[1, n-1]$.
4. Calculate the curve point $(x_1, y_1) = k \times G$.
5. Calculate $r = x_1 \bmod n$. If $r = 0$, go back to step 3.
6. Calculate $s = k^{-1}(z + rd_A) \bmod n$. If $s = 0$, go back to step 3.
7. The signature is the pair (r, s).

Verification process:

1. Verify that r and s are integers in $[1, n-1]$. If not, the signature is invalid.
2. Calculate $e = \mathrm{HASH}(m)$, where HASH is the same function used in the signature generation.
3. Let z be the L_n leftmost bits of e.
4. Calculate $w = s^{-1} \bmod n$.
5. Calculate $u_1 = zw \bmod n$ and $u_2 = rw \bmod n$.
6. Calculate the curve point $(x_1, y_1) = u_1 \times G + u_2 \times Q_A$.
7. The signature is valid if $r \equiv x_1 \pmod n$

Structure of ECDSA



5.OverallArchitecture

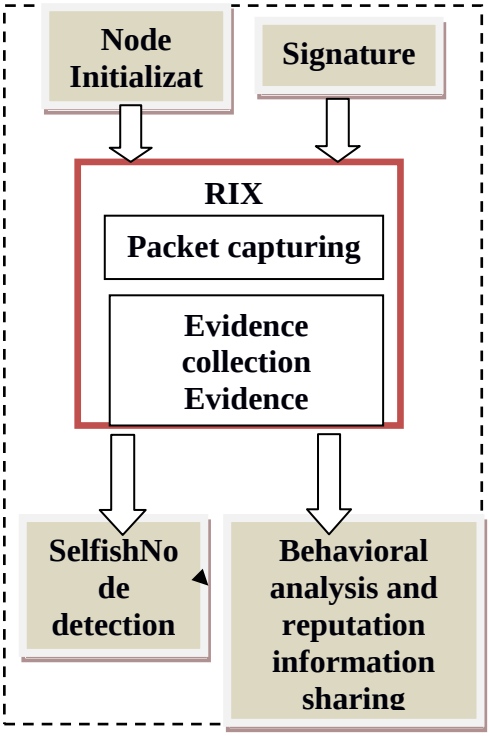


Fig 1.proposed model

6.Implementation and Results

The mean field reputation information sharing approach to detect the selfish nodes in NS2 Simulator and the number of nodes detected at different overhead, packet delay, delivery ratio, packet drop ratio is observed.

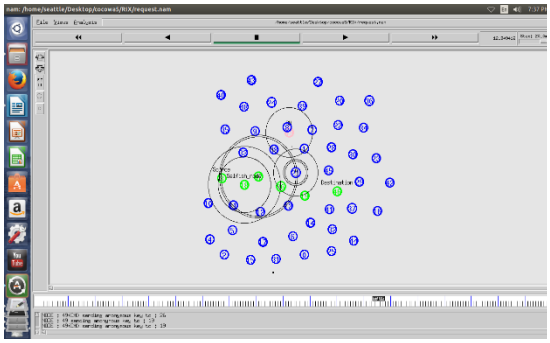


Fig 2. Simulation Result

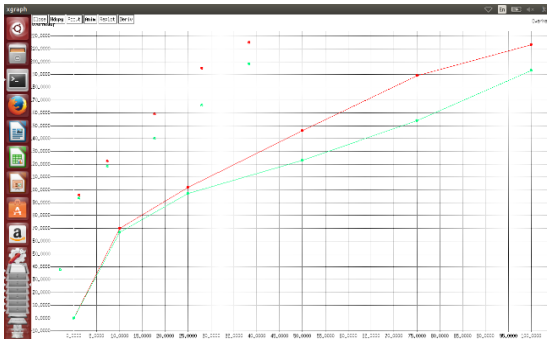


Fig 3.Overhead Graph

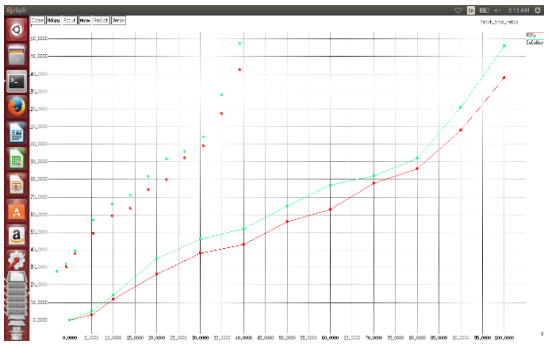


Fig 4. Packet Drop Ratio Graph

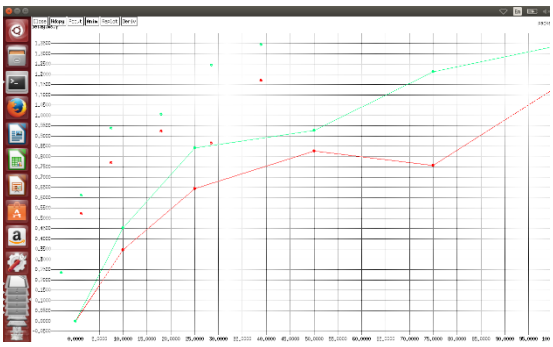


Fig 5. Packet Delay

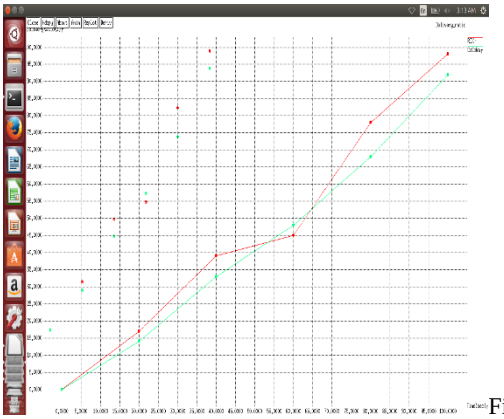


Fig 5.Delivery Ratio Graph

7.Conclusion

Node behaviour has maintained separately.Detection of selfish nodes are determined better than COCOWA.In each node transmission: key generation and verification are done.Security level, Authentication, Data integrity and non-reputation of nodes has been increased.RIX is based on the diffusion of positive and the negative acknowledgement.

References

[1]S.Abbas, M. Merabti,D. Llewellyn-Jones andK. Kifayat, "LightweightSybil attack detection in manets," IEEE Syst. J., vol. 7, no. 2, pp. 236–248, Jun. 2013.

[2]S. Bansal and M. Baker, "Observation- based cooperation enforcement in ad hoc networks" arXiv:cs.NI/0307012, 2003.

[3] S. Buchegger and J.-Y. Le Boudee,"Self-policing mobile ad hocnetworks by reputationsystems," IEEE.Mag., vol.43, Jul. 2005.

[4]L.Butty_and J.-P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in Proc. 1st Annu. Workshop Mobile Ad Hoc Netw. Comput., 2000, pp. 87–96.

[5]L.Butty_an and J.-P. Hubaux, "Stimulating cooperation in selforganizing mobile ad hoc networks," Mobile Netw. Appl., vol. 8,pp. 579–592, 2003.

[6] H. Cai and D. Y. Eun, "Crossing over the bounded domain: From exponential to power-law intermeeting time in mobile ad hocnetworks," IEEE/ACM Trans. Netw., vol. 17, no. 5, pp. 1578–1591,Oct. 2009.

[7] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott,"Impact of human mobility on opportunistic forwarding algorithms,"IEEE Trans. Mobile Comput., vol. 6, no. 6, pp. 606–620,Jun. 2007.

[8] J. R. Douceur, "The sybil attack," in Proc. Revised Papers

1st Int.Workshop Peer-to-Peer Syst., 2002, pp. 251–260.

[9] S. Eidenbenz, G. Resta, and P. Santi, "The COMMIT protocol for truthful and cost-efficient routing in ad hoc networks withselfish nodes," IEEE Trans. Mobile Comput., vol. 7, no. 1,pp. 19–33, Jan. 2008.

[10] W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in delay tolerant networks: A social network perspective," in Proc. 10th ACM Int.Symp. Mobile Ad Hoc Netw. Comput., 2009, pp. 299–308.