World Engineering & Applied Sciences Journal 7 (2): 68-73, 2016
ISSN 2079-2204
© IDOSI Publications, 2016
DOI: 10.5829/idosi.weasj.2016.7.2.22637

DTASR: Dual Threshold-based Authentication for Secure Routing in Mobile Adhoc Network

[1]*Burhan Ul Islam Khan,* [2]*Rashidah F. Olanrewaju,* [1]*Asifa Mehraj Baba,*
[3]*Roohie Naaz Mir and* [1]*Sajad Ahmad Lone*

[1]Department of Computer Science & Engineering, Islamic University of Science
and Technology, Awantipora, Kashmir, India
[2]Kulliyyah of Engineering, International Islamic University Malaysia, Kualalumpur, Malaysia
[1]Department of Electronics & Comm. Engineering,
Islamic University of Science and Technology, Awantipora, Kashmir, India
[3]Department of Computer Science & Engineering,
National Institute of Technology, Srinagar, Kashmir, India
[1]Department of Computer Science & Engineering,
Islamic University of Science and Technology, Awantipora, Kashmir, India

Abstract: The Mobile Adhoc Network (MANET) is not only limited to the temporary rescue operations rather it has been conceptualized to be adopted into many civil society comfort and safety applications. The self-configurability of MANET's node is the root cause of vulnerability and security threats, thus there is a need of light weight protocols which can ensure optimal Quality of Service (QoS) in secure way of routing. This paper projects a model of such secure routing in MANET called DTASR i.e. Dual Threshold-based Authentication for Secure Routing accentuating upon a resource-based threshold scheme as well as trust-based authentication scheme to ensure higher degree of resiliency against adversaries. The proposed illustrates an enhanced ability of communication performance when compared to conventional secure routing schemes.

Key words: Mobile Adhoc Network · Secure Routing · Authentication · Trust · Resource

INTRODUCTION

Mobile Adhoc Network consists of self-organizing nodes and is governed by highly decentralized architecture [1]. It is widely used in home and enterprise networking, tactical networks, commercial and civilian environment, emergency services, etc [2]. From more than a decade, there has been archives of literature that has spontaneously addresses the challenges and issues in MANET e.g. energy issues, routing issues, Quality of Service issue and security issues [3, 4]. Out of all the issues, security in MANET is still an unsolved problem owing to its inherent characteristics of dynamic topology, intermittent link breakage, as well as energy consumption [5, 6]. Although, there are various existing techniques to address security flaws in MANET [7], but few techniques were originally found to be highly resilient against potential adversaries in decentralized environment of MANET. The next section will highlight about the existing system and then the remaining of the paper focuses on the proposed novel solution towards security issues.

Existing Technqiues: This section discusses about some of the recent studies that have been carried out for securing the communication protocol in mobile adhoc network. In [8] the authors have significantly discussed and critically analyzed about the techniques used for addressing malicious behaviour of mobile nodes in adhoc network. Our second work [9] has introduced a novel framework that uses game theory for investigating the malicious behaviour as well as proposed a scheme to potentially resist the malicious activity of both selfish and malicious nodes. Apart from it, the other research papers that has been recently studied before designing the proposed system are highlighted in Table 1.

Corresponding Author: Burhan Ul Islam Khan, Department of Computer Science & Engineering,
Islamic University of Science and Technology, Awantipora, Kashmir, India.

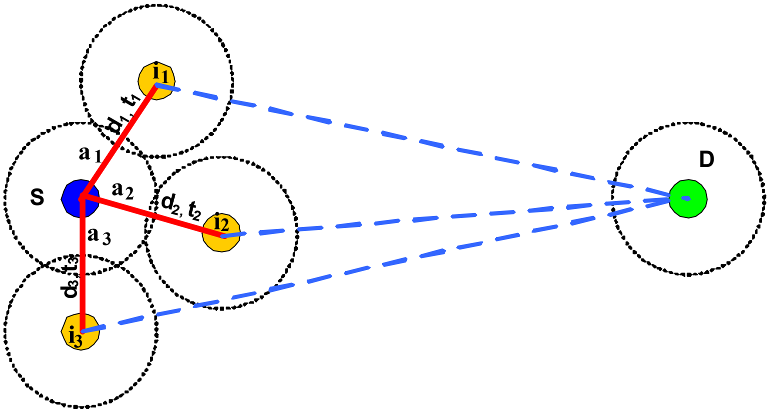

Fig. 1: Pictorial representation of Communication from S to D

Table 1: Recent Research work towards Security in MANET

Authors	Method Used and problem handled	Number of Citation	Remark
Marimuthu *et al* [10]	Enhanced OLRS, DoS Attack	12	Specific Solution for DOS attack
Venkataraman *et al* [11]	Regression based Trust, Secure Routing Protocol	6	Trust Model is used for Security
Lv *et al* [12]	Key Agreement Protocol, Secure group Communication	6	Secure group communication and small cipher text exploited for distributed applications
Zhang *et al* [13]	Lightweight Encryption Scheme, Network Coded	7	Lightweight Nature employed for minimal energy consumption
Zhao *et al.* [14]	IBC Security Applications, Applications of Identity-based Cryptography	36	IBC Security used for Mobile Adhoc Network
Dhanapal *et al.* [15]	Link quality-based cache replacement technique, Received Signal Strength	1	Cache replacement technique estimates used Received Signal Strength
Xi *et al.* [16]	Trust Management, Opportunistic Network	0	A Novel Trust Management used for information of behavior feedback

Research Methodology: The proposed study has considered the analytical modelling where the focus was laid not to use hard core cryptography for security purpose. The design and development of DTASR has primarily two core components i.e. i) design of resource-based thresholding scheme and ii) design principle of trust-based authentication scheme. Consider a source S intends to communicate to destination D with an availability of 3 neighbor nodes as illustrated in Fig. 1. The prime intention of the S would be to select the best neighbor node as well as the secure link that has got higher probability to reach destination D. The discussion of the core components of DTASR are as follows:

Design principle of Resource-based Thresholding Scheme: The prime aim of the threshold scheme is to select the best route where algorithm of inline authentication system can be implemented. However, in order to avail better performance of in-line authentication technique, the communicating node must have better mobility, enough bandwidth, minimum residual energy and a cut-off memory. Therefore, in route discovery process itself, DTASR enables S to compute probabilities (α_1, α_2, α_3,….) from its neighbor nodes (i_1, i_2, i_3, ….). These probabilities will be then compared with the threshold value T_α. Only, the nodes with probabilities more than T_α will be retained for next round of process while the node with lesser values of probabilities will be discarded.

The computation of the probability factor (α_1, α_2, α_3,….) was carried out by evaluating the shortest distance (d_1, d_2, d_3) as well as time (t_1, t_2, t_3) of intermediate hops (i_1, i_2, i_3, ….) with respect to total distance and time of the link proceeding towards the destination node D. In order to avoid generation of infinite loop, the computation for probability is only allowed to continue for a range of particular duration t. The mathematical representation of the objective function f(x) of DTASR can be thereby represented as follows,

$$f(x)=\sum_{n=1}^{N}\alpha_n[\forall\alpha_n \subseteq \arg_{\min}(d_n t_n)] \qquad (1)$$

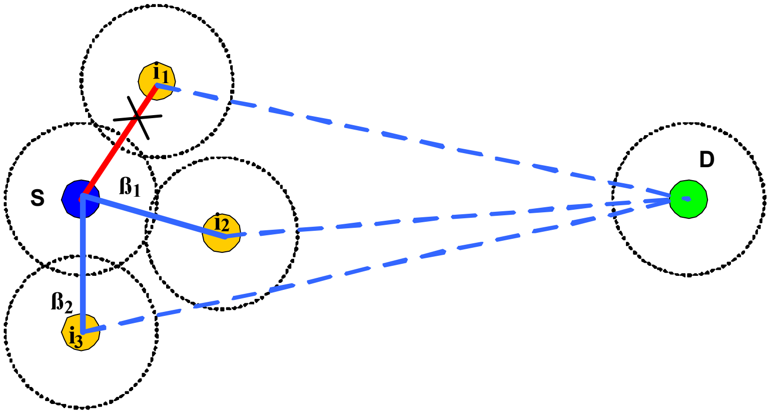

Fig. 2: Pictorial representation of In-line authentication system

Inline with the Equation (1), the objective function will look for first computing the values of probabilities (i.e. α) and then it sorts the probabilities based on the minimal value of probabilities of distance and time of hops.

Using a broadcasting mechanism the system assumes that routing information is equally disseminated proportionately resulting in the knowledge of the probabilities of distance and time in the memory. In case of fresh routing, the older memory of distance and time are then updated to the new only resulting in no memory overhead as well as precise update of routing. The threshold value of T_α is initialized in the preliminary phase, which is computed with respect to initial distance and time among each node. Using the broadcasting mechanism, the nodes get the updates of the prior threshold, which is then revised based on the communicating node requirements. The outcome of this technique is best value of objective function i.e. best routes with higher probability of reaching the destination early. DTASR then performs in-line authentication for only the communicating nodes compliant of objective function. Further discussion of this algorithm is carried out in Algorithm-1 in Section IV.

Design Principle of Trust-based Authentication Scheme: This mechanism mainly intends for performing in-line authentication among the nodes that are compliant of objective function discussed in eq.(1). Consider that the probability factor α_3 was found to be less than T_α and it therefore got discarded. Therefore, the routing will not be carried out with hop i_1. The source will choose to prefer routing using hops i_2 and i_3 as shown in Fig. 2. Also consider that (α_1, α_2) of hops i_2 and i_3 are more than $T_{\alpha.}$ This is the only favorable probability that node S will choose to perform routing. However, before, performing routing via these hops, it is also required to authenticate the hops. DTASR chooses to opt for another set of threshold T_β and probabilities β_1 and β_2 on hop i_2 and i_3 respectively. This threshold probability is designed based on state-based trust that incorporates discrete states of trust e.g. undeviating trust, suggested trust and Capacity of Transmitting (CoT). Hence, the hop with more value of β will be considered for secure routing of data packets from source S to destination D. However, if there are two value of β found to be more than threshold T_β than the system selects the hop with more residual energy, shortest distance and shortest travel time.

Therefore, DTASR perform routing by comparing its resource probability factor (α_1, α_2, α_3,….) with threshold T_α and then the selected hops are compared for its trust-based probability factor ($\beta_{1,}$ $\beta_{2,}$ $\beta_{3,.....}$) with threshold $T_{\beta.}$ The next section will present the discussion of algorithm implementation for both the scheme and will bring further insights to the potential factor of the algorithm design to ensure secure routing in mobile adhoc network.

Algorithm Implementation: The analytical design of DTASR is discussed briefly in this section with an aid of Algorithm-1 that performs resource-based thresholding scheme while Algorithm-2 performs trust based authentication (or thresholding) scheme. The simulation parameters will consist of 40-100 numbers of nodes using Random Waypoint Model with mobility of 0-30 m/s. The nodes are considered having a maximum range of transmission with 300 meters inline with 802.11 MAC protocol. Considering a simulation time of 1000 seconds, the simulation study is carried out in Matlab. The description of the core algorithms are as follows:

Algorithm-1: Algorithm for Resource-based Thresholding Scheme

```
Input: N (Total Number of nodes), $d_i$ (Transmission distance of neighbor node i), $d_S$ (Transmission distance of Source S), $d_{iS}$ (distance between i and S)
Output: Route with higher resource probability
Start:
1. Initialize number of nodes (N)
2. Apply Random mobility model
3. S→beacon→$i_n$
4. If $d_{Si} < (d_i + d_S)$
5.     S calculates $\alpha$ ($i_n$)
6. For round=0 to max(round)
7. $T_\alpha = g_{best}(d, t)$
6. if $\alpha(i_n)<T_\alpha$
7.     Discard $d_{Si}$
8. Or else
9.     Select min($d_{Si}$)
10. Apply Objective Function
        $f(x) = \sum_{n=1}^{N} \alpha_n [\forall \alpha_n \subseteq \arg_{\min}(d_n t_n)]$
10. f(x)→Apply Algorithm-2
End
```

Algorithm-1 takes the input of simulation parameters and applies random mobility model. A beacon is generated from source S that is received by intermediate hops (in, n=1, 2, …. N) as specified in Line-3. If both the nodes S and i falls within a transmission range of each other (Line-4) than S starts computing resource probabilities of intermediate nodes in and returns all the values to S (Line-5). For all the simulation iteration (Line-6), the resource-based threshold T_α is computed by global best result of distance and time for all the nodes leading from i and ends at D. (Line-7). The individual probability factor α will be computed for all the intermediate hopes (Line-8). In case the probability factor of intermediate hope $\alpha(i_n)$ are found less than threshold T_α, than the particular route (dSi) is discarded or else it is selected (Line 7 and 9). Finally, the objective function is applied on the selected routes to find the best routes. In case more than two routes are found to be more than T_α, the algorithm selects only the routes with lesser value of t from the input arguments to objective function.

Algorithm-2 takes the input of the objective function from the prior algorithm and it essentially computes to find the most secure route using trust-based thresholding (or authentication) scheme. The cumulative trust β is computed using empirical relationship expressed in Line-5 of Algorithm-2, where it can be seen that trust is computed from undeviated trust (δ_{ut}), suggested trust (δ_{sug}) and capacity of transmitting (CoT). The simulation study also consider some of the constraint factors for trust computation e.g. p, q and r, where p, q, r □ [0, 1] and p + q + r=1 owing to adoption of probability theory.

Algorithm-2: Algorithm for Trust-based Thresholding Scheme

```
Input: objective function (f(x)), p (probability), R (regular nodes), M (malicious nodes), $E_{res}$ (residual energy), bw(bandwidth).
Output: Route with higher trust probability
Start:
1. Select routes compliant of f(x)
2. Evaluate undeviated trust
    $\delta_{ut} = \begin{Bmatrix} \frac{p(R)-p(M)}{p(R)+p(R,M\}} & p(R)>p(M) \\ 0 \quad or-else & \end{Bmatrix}$
3. Evaluate suggested trust
    $\delta_{sug} = \begin{Bmatrix} p(R)-p(M), & p(R)>p(M) \\ 0 & or-else \end{Bmatrix}$
4. CoT = {$E_{res}$(i), bw(i), mobility state (i)}
5. Evaluate total trust $\beta$
    $\beta = \delta_{ut}(i,j).p + \delta_{sug}(i,j).q + CoT(j).r$
6. Initialize $T_\beta$=0.05
6. If $\beta<T_\beta$
7.     Discard $d_{Si}$
8. or else
9.     Select $d_{Si}$
10. Forward data packet
End
```

The first essential component is the computation of undeviated trust as shown in Line-2 above. We assume a straightforward fact that if an intermediate node assist in packet transmission that we term it as regular node or else malicious node. A closer look into the Line-2 will show that in order to calculate undeviated trust, it is essential to compute probability of regular node p(R), probability of malicious node p(M) and probability of unknown type of mobile node as p(R, M). Similarly, Line-3 represented the trust factor offered by other neighbor nodes for node S and node i. The last variable Capacity of Transmitting

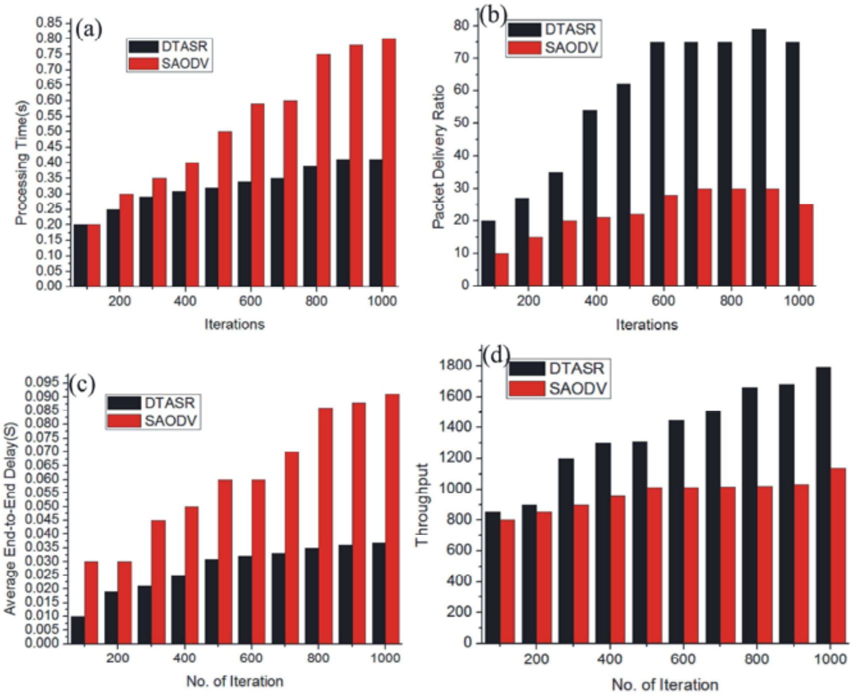

Fig. 3: Analysis of the Comparative performance Outcome of DTASR and SAODV

(CoT) is computed by evaluating amount of residual energy, bandwidth and mobility state of intermediate hops. The algorithm than computes the individual trust-based probability factor β of an intermediate hops and chooses only those hops which are found more than trust threshold T_β. For routes with more than two routes with probability value more than T_β., the system than randomly selects the probability factor and chooses to route data packets in the newly selected route.

RESULT AND DISCUSSION

The proposed system is compared with the standard secure routing protocol of SAODV [A]. Fig. 3 exhibits the outcome of the study that is evaluated with respect to performance parameters of processing time, packet delivery ratio, average end-to-end delay and throughput.

As per Fig.3(a), the performance of processing time of proposed DTASR is much lower compared to SAODV. From the viewpoint of packet delivery ratio and throughput in Fig.3(b) and Fig.3(d), DTASR excels better communication performance as compared to conventional SAODV. Fig.3(c) highlights that DTASR has better delay performance as compared to SAODV. The prime reason behind this is SAODV highly depends on sophisticated cryptographic operation for which purpose the resource consumption becomes too massive. Another bigger problem with SAODV is higher delay owing to spontaneous resists replying on behalf of receiver node. Moreover, the signature mechanism used in SAODV results in more computational time and doesn't yield much better throughput.

CONCLUSION

This paper has presented a secure mitigation policy to resist unauthorized access in Mobile adhoc network. In order to carry out this goal, the proposed system has adopted a non-cryptographic mechanism to retain maximum level of security using analytical modelling approach. With an aid of probability theory, the proposed system allows the node to evaluate the reliability of its adjacent nodes in order to find out jointly if i) if the neighbor nodes will lead to faster data communication and ii) if the routes created by intermediate hops have higher trust factor. The system spontaneously evaluates the trust factor and updates itself after every cycle of successful or failure authentication. The updated trust factor is then broadcasted in order to secure the other routes too. Hence, the resiliency towards any form of illegitimate access will be denied as such forms of malicious or unknown nodes will finally yield lower value of trust factor. The proposed system has used a threshold based mechanism, which is quite simple and yet robust with usage of static memory consumption of the routing updates. Hence, the technique discussed is both compliant of time complexity and memory complexity too. The outcome shows that proposed system excels better than conventional security technique in mobile adhoc network. Our future work will be further in the direction of enhancing the level of security and to compare it with more number of conventional techniques.

REFERENCES

1. Jin, M. and Z. Du, 2014. Management Innovation and Information Technology, WIT Press, 12-Jun-2014.
2. Sarkar, S.K., 2012. Wireless Sensor and Ad Hoc Networks Under Diversified Network Scenarios, Artech House.
3. Loo, J., J.L. Mauri and J.H. Ortiz, 2012. Mobile Ad Hoc Networks: Current Status and Future Trends, CRC Press.
4. Kennington, J., E. Olinick and D. Rajan, 2010. Wireless Network Design: Optimization Models and Solution Procedures, Springer Science & Business Media.
5. Amine Abdelmalek, 2013. Network Security Technologies: Design and Applications: Design and Applications, IGI Global.
6. Pathan, K., M.M. Monowar and Z.M. Fadlullah, 2013. Building Next-Generation Converged Networks: Theory and Practice, CRC Press.
7. Pathan, K., 2010. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, CRC Press,
8. Khan Islam, R.F. Olanrewaju and M.H. Habaebi, 2013. Malicious Behaviour of Node and its Significant Security Techniques in MANET-A Review, Australian Journal of Basic and Applied Sciences, 7(12): 286-293.
9. Khan Islam, R.F. Olanrewaju, R.N. Mir and B.W. Adebayo, 2015. Behaviour Visualization for Malicious-Attacker Node Collusion in MANET Based on Probabilistic Approach, American Journal of Computer Science and Engineering, 2(3): 10-19.
10. Marimuthu, M. and K. Ilango, 2013. Enhanced OLSR for defense against DOS attack in ad hoc networks, in Journla Communications and Networks, 15(1): 31-37.
11. Venkataraman, R., M. Pushpalatha and T.R. Rao, 2012. Regression-based trust model for mobile ad hoc networks, in Information Security, IET, 6(3): 131-140.
12. Lv, X. and H. Li, 2013. Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks, in Information Security, IET, 7(2): 61-66.
13. Zhang, P., C. Lin, Y. Jiang, Y. Fan and X. Shen, 2014. A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks, in IEEE Transactions on Parallel and Distributed Systems, 25(9): 2211-2221.
14. Zhao, S., A. Aggarwal, R. Frost and X. Bai, 2012.A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks, in IEEE Communications Surveys & Tutorials, 14(2): 380-400.
15. Dhanapal, J. and S.K. Srivatsa, 2013. Link quality-based cache replacement technique in mobile ad hoc network, in Information Security, IET, 7(4): 277-282.
16. Xi, S. Liang, M. Jianfeng and M. Zhuo, 2015. A trust management scheme based on behavior feedback for opportunistic networks, in Communications, China, 12(4): 117-129.