International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 2, Mar-Apr-2020, ISSN (Online): 2395-566X

Water Spider Monkey Optimization Algorithm for Trust-based MANET Secure Routing in IoT

Sunita Nandgave-Usturge[1,2]
Department of Computer Science and Engineering,
[1]G H Rasoni College of Engineering and Management, Pune
[2]Koneru Lakshmaiah Education Foundation,
Vaddeswaram, AP, India
Sunita.nandgave@raisoni.net

Dr. T Pavankumar
Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, AP, India
pavankumar_ist@kluniversity.in

***Abstract* – In Mobile Ad-hoc Network all nodes are moving continuously. Due to dynamic topology routing in MANET is challenging. Nodes are resource constraint so difficult to employ security solutions. Proposed security scheme has two phases, first phase is bi-filtering and other phase is routing. In bi-filtering phase different parameters are used such as direct trust, indirect trust, and historical trust etc. in identifying a secured node. Thus in bi-filtering phase important nodes are filter out for communication. The trust of the nodes evaluated and only the nodes with high trust factor involved in the secure communication using optimization, after identification of secure nodes in next phase routing is done by proposed hybrid optimization algorithm namely, Water Spider Monkey Optimization (WSMO). WSMO, which again finds the better path based on the trust and other factors, like distance, delay, and the overhead parameters so that the security will be further enhanced. This paper addresses a new optimization will be developed based on the WWO and SMO so that the routing in MANET shall be done for which the fitness will be the security factors of the nodes in the network.**

***Keywords* – MANET, DoS, Internet of Things, E2SR, WWO, SMO, WSMO.**

I. INTRODUCTION

Mobile Ad-hoc NETwork is a network of free and mobile nodes (devices) communicating in an ad hoc manner without the aid of any centralized administrative infrastructure like access points or base stations [5].

MANET is a typical dynamic, wireless network that has no infrastructure and central authority [9] [1] [10]. Security is a prime issue in MANET due to weak connectivity, resource constraints, and limited physical protection of the mobile nodes [3].

It is the major concern in MANET since absence of infrastructure involves many security threats [11] [1] [12]. In MANET, alteration, denial of service [29], Sybil attack [28], replay attack, fabrication attack, spoofing attack, Black hole attack [30] and jamming attack are frequently identified and considered to be harmful attacks. To mitigate these threats, MANETs require following security services: availability, authenticity, confidentiality, integrity, anonymity, non-repudiation, and privacy [1].

One of the fundamental driving forces of IoT is networking and particularly routing, which drives and facilitates the interconnection of devices [17] [5]. A major consideration during IoT routing is: scalability, autonomy and secure communication and energy efficiency [18] [5]. Rapid growth in wireless communication technologies supports the evolution of Internet of Things (IoTs) in many real-time applications, such as business applications, smart home applications, smart city applications, and so on [13] [14] [15] [1].

IoT comprises millions of physical devices/nodes that are capable to see, hear, and communicate with each other [1]. IoT applications are becoming smarter for various applications namely education, finance, energy, healthcare, transportation and smart cities [16] [4].

A.Secure routing is considered to be one of the solutions for securing communication in MANET environment [13] [1].

Reputation [21] [20] is formed by a node’s past behavior and reveals its cooperativeness. In secure routing, reputation mainly evaluates the routing and forwarding, the use of encryption and authentication mechanisms, and the proper transmission of acknowledgements per transmitted packets [20]. Many trust-based systems have been utilized to achieve secure routing [22] [20].

MANET takes network communication with available nodes and forming dynamic topology in nature and the nodes are so much resource constraint that it is difficult to employ security solutions [10].

Trust-based routing [23] [1] and lightweight cryptography [24] [1] techniques also enhance the security in MANET environment. The trust evaluation techniques identify the behavioural pattern of the nodes, whereas cryptography techniques ensure the security for transmitted data. A threshold cryptography technique is used to share the secret key and finally the shares can be reconstructed by using Lagrange interpolation method [11].

1. **Literature Review:** This section depicts a review of the literature on various existing MANET secure routing in IoT. These research papers are taken and reviewed according to the recent published years based on MANET secure routing in IoT techniques.

2. **Challenges:**

- In [1], Energy efficient secure routing (E2-SR) scheme is developed for MANET secure routing in IoT, but failed to minimize delay and design large-scale MANET-IoT environment with security and energy efficiency.
- In [4], a secure routing and monitoring protocol with multi-variant tuples using Two-Fish (TF) symmetric key approach is introduced. Although, a real time validation and IoT-based Wireless Sensor Network is not applied to authenticate the secrecy of application environment.
- In [5], Secure Trust-Aware RPL Routing Protocol is developed for MANET secure routing in IoT. However, failed to improve the integration of trusted nodes into the network that have recoupled their battery power.
- In [9], a discrete-event simulation model of an ad-Hoc network secure routing in IoT is developed. However, prediction methods are not applied to evaluate network traffic in order to improve dimensioning.
- In [23], Refined Trust Energy-Ad Hoc on Demand Distance Vector (ReTE-AODV) routing algorithm is developed for secure routing in MANET. However, the method failed to use intelligent rules to make effective decisions in routing.

II. THE PROPOSED METHODOLOGIES

The primary intention of this research is to design and develop trust-based MANET secure routing in IoT, where the IoT nodes are placed in mobile ad-hoc manner. The phases followed in the developed model will be secure node identification phase, Bi-filtering phase and the Routing phase. In the secure node identification phase, the parameters such as, Direct trust, Indirect trust, Historical trust and Fuzzy-based aggregation mechanisms will be considered for identifying the secure nodes. Then, the communication and network-based parameters will be considered in the bi-filtering phase in order to filter out the important nodes. After the identification of important nodes, the routing will be carried out based on the proposed hybrid optimization algorithm. Trust, distance, delay, and the overhead parameters will be the two parameters considered in this proposed work.

Based on these parameters, the routing model, named Water Spider Monkey Optimization (WSMO) will be introduced. The WSMO will be designed newly by combining Water Wave Optimization (WWO) algorithm [25] and Spider Monkey optimization (SMO) [26].
Spider Monkey Optimization Algorithm is intelligent behaviors from the natural world [5].

- **WSMO hybrid Algorithm:**

Proposed WSMO hybrid algorithm uses both principle of Water wave optimization and Spider Monkey Optimization (searching of food).
WSMO is based on searching next secured neighbor node in routing process.
Step 1. Initialize the community, Assume that n number of neighbor nodes are available in the network.
Step 2. Calculate path to destination node (means distance of the food sources).
Step 3. Using a greedy selection to select leaders (Minor and Major)
Step 4. While (path to destination do not met) do
Step 5. To find the goal path to destination ,
Step 6. Compute the trust of next node
Step 7. If trust value of next node is above threshold then it’s a secure node else ignore this node and goto step 3.
Step 8. Now we got new secure node in all group members selected by initial node, with the help of trust value.
Step 9. Now routing process starts
Step 10. Then update the value of Minor Leader and Major Leader by applying the greedy selection process.
Step 11. If a Minor Leader group does not update his location of neighbor after specific number of times (LLlimit), then he redirects all the group members for algorithmic feeding.
Step 12. Now Major Leader does not update his neighbor node location for a specific no. of times (MLlimit), that divide the groups.
Divide the population into groups.
else
merge all groups
Update neighbor position.

The block diagram of the trust-based MANET secure routing in IoT using Water spider monkey Optimization is depicted in figure 1. The implementation of the proposed approach will be done using NS2. The performance of the proposed method will be analyzed using three performance metrics, namely through put, Delay, packet delivery ratio by considering without attack and with attack, such as black hole, denial of service, sink hole effect, and the results will be compared with that of the existing works [1], and [3].

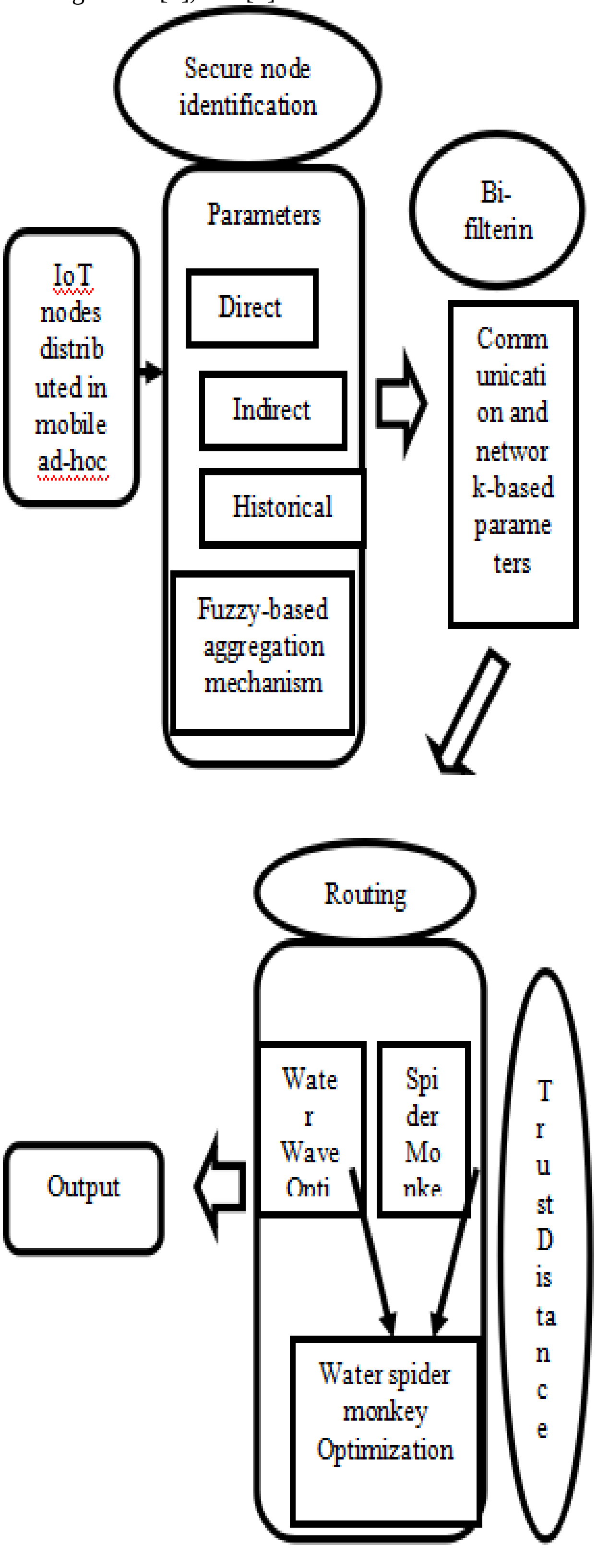
Secure node identification
Parameters
IoT nodes distributed in mobile ad-hoc
Direct
Indirect
Historical
Fuzzy-based aggregation mechanism
Bi-filterin
Communication and network-based parameters
Routing
Water Wave Opti
Spider Monke
Water spider monkey Optimization
Trust Distance
Output

Fig.1.Trust-based MANET secure routing in IoT using Water spider monkey Optimization.

Table –I: Comparison of various security method.

Methods	Advantages	Disadvantages
Energy efficient secure routing (E2-SR) scheme [1]	Improves the overall network performance in security as well as in data transmission.	Credibility score computation performed by a node itself is not efficient for secure network environment.
Trusted Routing Scheme[2][27]	In order to improve the quality-of-services, this method intended to isolate the adversaries at an early stage.	Failed to strengthen the security along with enhancing network capacity.
Novel quantitative trust model [3]	Packet delivery fraction decreases with the increased number of malicious nodes for all the protocols.	Failed to consider direct trust evidence and collected recommendation evidences to minimize the malicious attacks.
A secure routing and monitoring protocol with multi-variant tuples using Two-Fish (TF) symmetric key approach[4]	Provide a low-level insightful operation to examine the network topology.	Other ns-versions are not considered to manage or negotiate a traffic pattern of end-to-end connectivity to control the network load.
Secure Trust-Aware RPL Routing Protocol[5]	Used to detect and isolate attacks while optimizing network performance.	Failed to address other colluding attacks like Rank/Black hole, Rank/Sybil, Rank/Selective Forwarding attacks.
Trust based routing mechanism[6]	Redundant multipoint relays provide more choices for selecting routes.	Suffers from many serious security threats

Energy efficient and secure routing protocol[7]	To achieve a secure network-wide data routing against malicious nodes a light-weight secret sharing scheme is adapted between cluster heads and base station.	Failed to consider multi-hop network communication along with the mobility standards.
Routing solution for the IoT system using a combination of MANET protocols and WSN routing principles[8]	By use of dynamical cluster head selection, sensor lifetime in the overall IoT system will increase.	The consumption of energy distribution is unbalanced in the network and observable the weakness network location.

III. CONCLUSION

As a result of our studies, it can be said that we can increase the performance of MANET node routing security. Water Spider Monkey Optimization technique used to search secured nodes to protect route as well as messages transmitted during communication. Trust based scheme are useful to provide secure routing functionality. Proposed WSMO scheme has bifiltering phase where secure nodes collected and routing phase for communication between secure nodes. The performance of Proposed WSMO protocol can be analyzed using performance metrics namely throughput, delay, packet delivery ratio by considering without attack and with attack such as blackhole, Denial of Service etc. results will be comapared with existing work.

REFERENCES

[1]. Ponguwala, Maitreyi, and Sreenivasa Rao, "E2-SR: a novel energy-efficient secure routing scheme to protect MANET-IoT", IET Communications, vol.13, no.19, pp.3207-3216, September 2019.

[2]. Jhaveri, Rutvij H., Narendra M. Patel, Yubin Zhong, and Arun Kumar Sangaiah, "Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT, IEEE Access, vol.6, pp.20085-20103, April 2018.

[3]. Alnumay, Waleed, Uttam Ghosh, and Pushpita Chatterjee, "A Trust-Based predictive model for mobile ad hoc network in internet of things", Sensors, vol.19, no.6, pp.1467, January 2019.

[4]. Deebak, B. D., and Fadi Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks", Ad Hoc Networks, vol.97 pp.102022, February 2020.

[5]. Airehrour, David, Jairo A. Gutierrez, and Sayan Kumar Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things", Future Generation Computer Systems, vol. 93, pp.860-876, April 2019.

[6]. Tan, Shuaishuai, Xiaoping Li, and Qingkuan Dong, "Trust based routing mechanism for securing OSLR-based MANET", Ad Hoc Networks vol.30, pp.84-98, July 2015.

[7]. Haseeb, Khalid, Ahmad Almogren, Naveed Islam, Ikram Ud Din, and Zahoor Jan, "An Energy-Efficient and Secure Routing Protocol for Intrusion Avoidance in IoT-Based WSN", Energies, vol.12, no.21, pp.4174, January 2019.

[8]. Alameri, I. A, "MANETS and internet of things: the development of a data routing algorithm", Engineering, Technology & Applied Science Research, vol.8, no.1, pp.2604-2608, February 2018.

[9]. Leite, JR Emiliano, Edson L. Ursini, and Paulo S. Martins, "Simulation of AdHoc networks including clustering and mobility", In International Conference on Ad-Hoc Networks and Wireless Springer, pp.199-209, September 2017.

[10]. Kumar, V. Vinoth, and S. Ramamoorthy, "Secure adhoc on-demand multipath distance vector routing in MANET", In Proceedings of the International Conference on Computing and Communication Systems Springer, pp.49-63, 2018.

[11]. Balasubramani, S., S. K. Rani, and K. Suja Rajeswari, "Review on Security Attacks and Mechanism in VANET and MANET", In Artificial Intelligence and Evolutionary Computations in Engineering Systems Springer, pp. 655-666, 2016.

[12]. Liu, Gao, Zheng Yan, and Witold Pedrycz, "Data collection for attack detection and security measurement in mobile ad hoc networks: A survey", Journal of Network and Computer Applications, vol.105, pp.105-122, March 2018.

[13]. Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications", IEEE communications surveys & tutorials, vol.17, no.4, pp.2347-2376, June 2015.

[14]. Ray, Partha Pratim, "A survey on Internet of Things architectures", Journal of King Saud University-Computer and Information Sciences, vol.30, no.3, pp.291-319, July 2018.

[15]. Lin, Jie, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications", IEEE Internet of Things Journal, vol.4, no.5, pp.1125-1142, March 2017.

[16]. Medagliani P, Leguay J, Duda A, Rousseau F, Duquennoy S, Raza S, Ferrari G, Gonizzi P, Cirani S, Veltri L, Monton M, "Internet of things applications-from research and innovation to market deployment" 2014.

[17]. Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac, "Internet of things: Vision, applications and research challenges", Ad hoc networks, vol.10, no.7, pp.1497-1516, September 2012.

[18]. Hui, Terence KL, R. Simon Sherratt, and Daniel Díaz Sánchez, "Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies", Future Generation Computer Systems, vol.76, pp.358-369, November 2017.

[19]. Karlof, Chris, and David Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Ad hoc networks, vol.1, no.2-3, pp.293-315, September 2003.

[20]. Hatzivasilis, George, Ioannis Papaefstathiou, and Charalampos Manifavas. "SCOTRES: secure routing for IoT and CPS", IEEE Internet of Things Journal, vol.4, no.6, pp. 2129-2141, September 2017.

[21]. Hatzivasilis, George, and Charalampos Manifavas, "Building trust in ad hoc distributed resource-sharing networks using reputation-based systems", In 2012 16th Panhellenic Conference on Informatics IEEE, pp.416-421, October 2012.

[22]. Dalal, Renu, Manju Khari, and Yudhvir Singh, "Survey of trust schemes on ad-hoc network", In International Conference on Computer Science and Information Technology Springer, pp.170-180, January 2012.

[23]. Sethuraman, Priya, and N. Kannan, "Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET", Wireless Networks, vol.23, no.7, pp.2227-2237, October 2017.

[24]. Reshmi, T. R., and K. Murugan, "Light weight cryptographic address generation (LW-CGA) using system state entropy gathering for IPv6 based MANETs", China Communications, vol.14, no.9, pp.114-126, October 2017.

[25]. Zheng, Yu-Jun, "Water wave optimization: a new nature-inspired metaheuristic," Computers & Operations Research, vol.55, pp. 1-11, 2015.

[26]. Bansal, Jagdish Chand, Harish Sharma, Shimpi Singh Jadon, and Maurice Clerc, "Spider monkey optimization algorithm for numerical optimization", Memetic computing, vol.6, no.1, pp.31-47, March 2014.

[27]. Banoth Rajkumar , Dr. G. Narsiimha , "Trust based certificate revocation for seure routing in MANET", In International Conference on Intelligent Computing, Communication & Convergence, published by Elsevier , Science Direct 2016, 431-441.

[28]. Kannan Govindan, member IEEE and Prashant Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A survey", 2012 IEEE communication surveys & Tutorial, Vol. 14, No. 2, Second Quarter 2012.

[29]. Rutuij H. Jhaveri, Sankita J Patel, Devesh C. Jinwala, "DoS Attacks in Mobile Adhoc Networks: A survey", 2012 Second International Conference on Advanced Computing & Communication Technologies IEEE 2012.

[30]. Arvind Dhaka, Amita Nandal and Raghuveer S. Dhaka, "Gray and Blackhole Attack Identification using Control Packets in MANETs", ScienceDirect, Procedia Computer Science 54(2015) (IMCIP 2015).