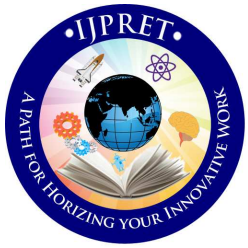
Research Article *ISSN: 2319-507X*
Shekar TP, IJPRET, 2013; Volume 1(8): 521-529 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

RISK-AWARE MITIGATION FOR MANET USING DEMPSTER – SHAFER THEORY BY CONSIDERING PERFORMANCE MATRICS

T. P. SHEKAR[1], PRASHANT D. KHANDALE[2], SAKEEB H. SHEIKH[3]

1. Associate prof., Department of Computer Science & Engineering, Vivekanand Institute of Technology & Science, Karimnagar, Jawaharlal Nehru Technological University, Hyderabad
2. M-tech, Department of Computer Science & Engineering, Vivekanand Institute of Technology & Science, Karimnagar, Jawaharlal Nehru Technological University, Hyderabad
3. B. E. Department of Computer Engineering, Maharashtra.

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Manets,

Risk mitigation,

Attacks,

Risk-aware approaches

Corresponding Author

Mr. T. P. Shekar

Abstract

Mobile Ad hoc Networks (MANET) are proven network but due to its dynamic nature highly affected with attacks. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. Even though there exist several intrusion response techniques to mitigate such critical attacks, existing solutions typically attempt to isolate malicious nodes based on binary or naı¨ve fuzzy response decisions. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and naı¨ve fuzzy responses could lead to uncertainty in countering routing attacks in MANET. In this paper, we propose a risk-aware response mechanism to systematically cope with the identified routing attacks. Our risk-aware approach is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of importance factors. In addition, our experiments demonstrate the effectiveness of our approach with the consideration of several performance metrics.

INTRODUCTION

Risk-aware approaches. When it comes to make response decisions [2], [3], there always exists inherent uncertainty which leads to unpredictable risk, especially in security and intelligence arena. Risk-aware approaches are introduced to tackle this problem by balancing action benefits and damage trade-offs in a quantified way. Cheng et al. [3] presented a fuzzy logic control model for adaptive risk-based access control. Teo et al. [4] applied dynamic risk-aware mechanism to determine whether an access to the network should be denied or permitted. However, risk assessment is still a nontrivial challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning. Wang et al. [4] proposed a naı¨ve fuzzy cost-sensitive intrusion response solution for MANET. Their cost model took subjective knowledge and objective evidence into account but omitted a seamless combination of two properties with logical reasoning. Mu et al. [7] adopted Dempster-Shafer theory to measure the risk of attacks and responses. However, as identified in [8], their model with Dempster's rule treats evidences equally without differentiating.

POTENTIAL RISK TREATEMENTS

From wikis Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:

- Avoidance (eliminate, withdraw from or not become involved)
- Reduction (optimize – mitigate)
- Sharing (transfer – outsource or insure)
- Retention (accept and budget)

Ideal use of these strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organization or person making the risk management decisions. Another source, from the US Department of Defense (see link), Defense Acquisition University, calls these categories ACAT, for Avoid, Control, Accept, or Transfer. This use of the ACAT acronym is reminiscent of another ACAT (for Acquisition Category) used in US Defense industry procurements, in which Risk Management figures prominently in decision making and planning.

RISK AVOIDANCE

This includes not performing an activity that could carry risk. An example would be not buying a property or business in order to not take on the legal liability that comes with it. Another would be not flying in order not to take the risk that the airplane were to be hijacked. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits.

HAZARD PREVENTION

Hazard prevention refers to the prevention of risks in an emergency. The first and most effective stage of hazard prevention is the elimination of hazards. If this takes too long, is too costly, or is otherwise impractical, the second stage is mitigation.

RISK REDUCTION

Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. For example, sprinklers are designed to put out a fire to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable. Halon fire suppression systems may mitigate that risk, but the cost may be prohibitive as a strategy. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied. By an offshore drilling contractor effectively applying HSE Management in its organization, it can optimize risk to achieve levels of residual risk that are tolerable.[9]

Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project. By developing in iterations, software projects can limit effort wasted to a single iteration.

Outsourcing could be an example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks.[10] For example, a company may outsource only its software development, the manufacturing of hard goods, or customer support needs to another company, while handling the

business management itself. This way, the company can concentrate more on business development without having to worry as much about the manufacturing process, managing the development team, or finding a physical location for a call center.

RISK SHARING

Briefly defined as "sharing with another party the burden of loss or the benefit of gain, from a risk, and the measures to reduce a risk."

The term of 'risk transfer' is often used in place of risk sharing in the mistaken belief that you can transfer a risk to a third party through insurance or outsourcing. In practice if the insurance company or contractor go bankrupt or end up in court, the original risk is likely to still revert to the first party. As such in the terminology of practitioners and scholars alike, the purchase of an insurance contract is often described as a "transfer of risk." However, technically speaking, the buyer of the contract generally retains legal responsibility for the losses "transferred", meaning that insurance may be described more accurately as a post-event compensatory mechanism. For example, a personal injuries insurance policy does not transfer the risk of a car accident to the insurance company. The risk still lies with the policy holder namely the person who has been in the accident. The insurance policy simply provides that if an accident (the event) occurs involving the policy holder then some compensation may be payable to the policy holder that is commensurate to the suffering/damage.

Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is different from traditional insurance, in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

RISK RETENTION

Involves accepting the loss, or benefit of gain, from a risk when it occurs. True self insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by

default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

EXISTING APPROACHES

Several work addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET scenario, improper counter measures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated. The notion of risk can be adopted to support more adaptive responses to routing attacks in MANET. Subjective knowledge could be retrieved from previous experience and objective evidence could be obtained from observation while logical reasoning requires a formal foundation. Wang et al. proposed a naı¨ve fuzzy cost-sensitive intrusion response solution for MANET. Their cost model took subjective knowledge and objective evidence into account but omitted a seamless combination of two properties with logical reasoning.

DISADVANTAGES

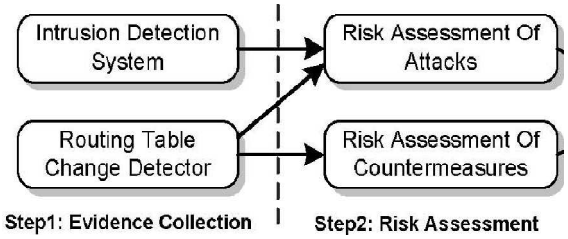
However, risk assessment is still a nontrivial, challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning.

PROPOSED SYSTEM

We formally propose an extended D-S evidence model with importance factors and articulate expected properties for Dempster's rule of combination with importance factors (DRCIF). Our Dempster's rule of combination with importance factors is nonassociative and weighted, which has not been addressed in the literature.

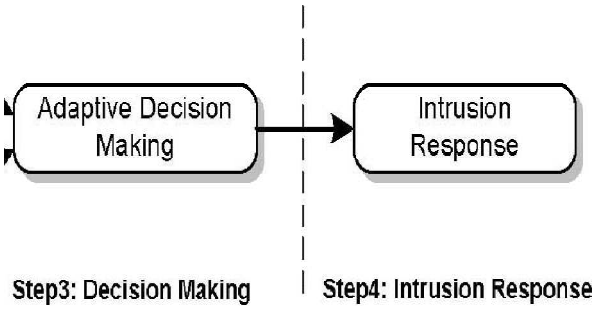
We propose an adaptive risk-aware response mechanism with the extended D-S evidence model, considering damages caused by both attacks and countermeasures. The adaptiveness of our mechanism allows us to systematically cope with MANET routing attacks.

We evaluate our response mechanism against representative attack scenarios and experiments. Our results clearly demonstrate the effectiveness and scalability of our risk-aware approach.



RISK - AWARE RESPONSE MECHANISM

In this section, we articulate an adaptive risk-aware response mechanism based on quantitative risk estimation and risk tolerance. Instead of applying simple binary isolation of malicious nodes, our approach adopts an isolation mechanism in a temporal manner based on the risk value. We perform risk assessment with the extended D-S evidence theory introduced in Section 3 for both attacks and corresponding countermeasures to make more accurate response decisions.



Des	Next	Dis
1	4	2
2	4	2
3	4	3
4	4	1
5	4	3
6	4	3

Before attack

Des	Next	Dis
1	1	1
2	1	2
3	1	3
4	4	1
5	1	2
6	1	2

After attack

Des	Next	Dis
2	4	2
3	4	3
4	4	1
5	4	3

After isolation

(a) Routing Table of Node 0

Risk-aware approaches. When it comes to make response decisions [2], [3], there always exists inherent uncertainty which leads to unpredictable risk, especially in security and intelligence arena. Risk-aware approaches are introduced to tackle this problem by balancing action benefits and damage trade-offs in a quantified way. Cheng et al. [3] presented a fuzzy logic control model for adaptive risk-based access control. Teo et al. [4] applied dynamic risk-aware mechanism to determine whether an access to the network should be denied or permitted. However, risk assessment is still a nontrivial challenging problem due to its involvements of subjective knowledge,

objective evidence, and logical reasoning. Wang et al. [4] proposed a naı¨ve fuzzy cost-sensitive intrusion response solution for MANET. Their cost model took subjective knowledge and objective evidence into account but omitted a seamless combination of two properties with logical reasoning. Mu et al. [7] adopted Dempster-Shafer theory to measure the risk of attacks and responses. However, as identified in [8], their model with Dempster's rule treats evidences equally without differentiating

Approaches

- Evidence collection.
- Risk assessment.
- Decision making.
- Intrusion response.
- Routing table recovery.

1) Evidence collection

In this step, Intrusion Detection System (IDS) gives an attack alert with a confidence value, and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack.

2) Risk assessment

Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated as well during a risk assessment phase. Based on the risk of attacks and the risk of countermeasures, the entire risk of an attack could be figured out.

3) Decision making

The adaptive decision module provides a flexible response decision-making mechanism, which takes risk estimation and risk tolerance into account. To adjust temporary isolation level, a user can set different thresholds to fulfill her goal.

4) Intrusion response

With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner.

5) Routing table recovery

Routing table recovery is an indispensable response and should serve as the first response method after successful detection of attacks. In proactive routing protocols like OLSR, routing table recovery does not bring any additional overhead since it periodically goes with routing control messages. Also, as long as the detection of attack is positive, this response causes no negative impacts on existing routing operations.

CONCLUSION

We have proposed a risk-aware response solution for mitigating MANET routing attacks. Especially, our approach considered the potential damages of attacks and countermeasures. In order to measure the risk of both attacks and countermeasures, we extended Dempster-Shafer theory of evidence with a notion of importance factors. Based on several metrics, we also investigated the performance and practicality of our approach and the experiment results clearly demonstrated the effectiveness and scalability of our risk aware approach. Based on the promising results obtained through these experiments, we would further seek more systematic way to accommodate node reputation and attack frequency in our adaptive decision model.

REFERENCES

1. Zhao Et Al.: Risk-Aware Mitigation For Manet Routing Attacks, Ieee Transactions On Dependable And Secure Computing, Vol. 9, No. 2, March/April 2012.

2. G. Shafer, A Mathematical Theory of Evidence. Princeton Univ., 1976.

3. L. Sun, R. Srivastava, and T. Mock, “An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions,” J. Management Information Systems, vol. 22, no. 4, pp. 109-142, 2006.

4. Mu, X. Li, H. Huang, and S. Tian, “Online Risk Assessment ofIntrusion Scenarios Using D-S Evidence Theory,” Proc. 13th European Symp. Research in Computer Security (ESORICS ’08),pp. 35-48, 2008.

5. K. Sentz and S. Ferson, “Combination of Evidence in Dempster- Shafer Theory,” technical report, Sandia Nat’l Laboratories, 2002.

6. L. Zadeh, “Review of a Mathematical Theory of Evidence,” AI Magazine, vol. 5, no. 3, p. 81, 1984.

7. R. Yager, "On the Dempster-Shafer Framework and New Combination Rules_1," Information Sciences, vol. 41, no. 2, pp. 93- 137, 1987.

8. H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor Fusion Using Dempster-Shafer Theory," Proc. IEEE Instrumentation and Measurement Technology Conf., vol. 1, pp. 7-12, 2002.

9. T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003.

10. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group,vol. 3561, 2003.

11. H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

12. Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 28- 39, May/June 2004.

13. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad Hoc Networks,vol. 1, nos. 2/3, pp. 293-315, 2003.

14. M. Yamada and M. Kudo, "Combination of Weak Evidences byD-S Theory for Person Recognition," Knowledge-Based Intelligent Information and Engineering Systems, pp. 1065-1071, Springer, 2004.

15. K. Fall and K. Varadhan, "The NS Manual," 2010.

16. F. Ros, "UM-OLSR Implementation (version 0.8.8) for NS2,"