Fakultät Informatik

Bewertung bekannter Ad-hoc-Routing-Protokolle zur prototypischen Realisierung einer mobilen Messenger-Applikation

Wissenschaftliches Schreiben im Studiengang Informatik

vorgelegt von

Jan-Eric Gedicke

Matrikelnummer 3653446

Erstgutachter: Marcus Fiebig

Zweitgutachter:

Inhaltsverzeichnis

1 Textzusammenfassung

Im Artikel *A Survey of Secure Mobile Ad Hoc Routing Protocols* wird gezeigt, dass Sicherheitsaspekte bei Ad-hoc-Routing-Protokollen für mobile Netzwerke eine zentrale Rolle spielen und in welchen Situationen Ad-hoc-Routing sogar internetbasierten Messenger-Applikationen überlegen ist [6, S. 1]. Der Artikel beschreibt die gängigsten Ad-hoc-Routing-Protokolle, AODV, DSR, OLSR, TORA, ihre Einteilung in reaktiv (on-demand), proaktiv (table-driven) und eine hybride Version beider, ihre grobe Verhaltensweise [6, S. 2] sowie die Sicherheitsbedrohungen, denen sie durch Angriffe wie Black-Hole-, Wormhole- oder Sybil-Angriffe ausgesetzt sind, und welche Methoden geeignet sind, diese Schwachstellen zu beheben [6, S. 4-11].

Einige Methoden sind kryptografische Verfahren, Intrusion Detection Systems (IDS) und Trust-basierte Mechanismen und es wird darauf eingegangen, inwiefern sie die Sicherheit erhöhen können, ohne die Leistung des Netzwerks signifikant zu beeinträchtigen [6, S. 7].

Das Besondere an diesem Textausschnitt ist die systematische Analyse bestehender Sicherheitslücken und die Diskussion potenzieller Lösungen für mobile Ad-hoc-Netzwerke [6, S. 9]. Nach wie vor offen ist das Problem, unter welchen Bedingungen neue Sicherheitsmechanismen implementiert werden können, die sowohl skalierbar als auch effizient sind [6, S. 12]. Folgende Fragen lässt Abusalah et al. jedoch offen: Wie können zukünftige Protokolle nicht nur sicher, sondern auch ressourcenschonend gestaltet werden, um den Einsatz in realen Anwendungen wie mobilen Messenger-Applikationen zu ermöglichen?

Darüber hinaus wird die Bedeutung von Vertrauen in der Sicherheit von MANETs hervorgehoben. Die Autoren betonen, dass Vertrauen eine wachsende Rolle spielt, insbesondere in offenen Umgebungen, in denen unbekannte Geräte jederzeit dem Netzwerk beitreten oder es verlassen können [6, S. 13]. Schließlich wird darauf hingewiesen, dass bestehende Verschlüsselungsmechanismen oft zu ressourcenintensiv sind und daher nicht immer praktikable Lösungen darstellen [6, S. 14]. Die Arbeit schließt mit der Empfehlung, zukünftige Forschungen auf die Entwicklung leichterer und effizienterer Sicherheitsmechanismen zu konzentrieren.

Ein weiterer wichtiger Aspekt, den die Autoren hervorheben, ist die Notwendigkeit, Ad-hoc-Netzwerke an spezifische Anwendungsszenarien anzupassen, um eine optimale

Balance zwischen Sicherheit und Leistung zu gewährleisten. Dabei wird auch auf die Bedeutung von Synergien zwischen Routing-Protokollen und Sicherheitsmechanismen eingegangen, um Bedrohungen proaktiv zu adressieren. Schließlich wird argumentiert, dass eine stärkere Integration von Lernmechanismen in Routing-Protokolle einen vielversprechenden Ansatz für die zukünftige Entwicklung darstellen könnte [6, S. 15].

2 Priorisierung der Literatur

Der Artikel *A Survey of Secure Mobile Ad Hoc Routing Protocols* [7] ist besonders wichtig, weil er eine umfassende Analyse von Routing-Protokolle, einen Fokus auf Sicherheitsanforderungen und einen Einblick in die Protokoll-Optimierung liefert.

Der Artikel *Ad Hoc Network based Android Messaging Apps* [12] ist besonders wichtig, weil er Fokus auf Ad-Hoc in Android-Plattformen und ihre praktischen Umsetzung eingeht.

3 Literaturverzeichnis

[1] Ikram Ali, Yong Chen, Mohammad Faisal, and Meng Li. *Efficient and Provably Secure Schemes for Vehicular Ad-Hoc Networks*. Springer, 2022.

[2] Driss Benhaddou and Ala Al-Fuqaha (Hrsg.). *Wireless Sensor and Mobile Ad-Hoc Networks: Vehicular and Space Applications*. Springer, 2015.

[3] S. Chatterjee and S. Das. Ant colony optimization based enhanced dynamic source routing algorithm for mobile ad-hoc network. *Information Sciences*, 295:67–90, 2015.

[4] Ana Juan Ferrer. *Beyond Edge Computing: Swarm Computing and Ad-Hoc Edge Clouds*. Springer Nature, 2023.

[5] William Roshan Quadros (Hrsg.), editor. *Proceedings of the 20th International Meshing Roundtable*. Springer-Verlag, 2011.

[6] X. Li, A. Nayak, I. Ryl, and D. Simplot. On secure mobile ad hoc routing. *Ad Hoc & Sensor Wireless Networks*, 4(3):229–254, 2007.

[7] Xiang-Yang Li, Symeon Papavassiliou, and Stefan Ruehrup (Hrsg.). Ad-hoc, mobile, and wireless networks: 11th international conference, adhoc-now 2012, belgrade, serbia, july 9-11, 2012. In *Ad-hoc, Mobile, and Wireless Networks: 11th International Conference, ADHOC-NOW 2012*. Springer, 2012.

[8] Muhammad Zeeshan Shakir, Muhammad Ali Imran, Khalid A. Qaraqe, Mohamed-Slim Alouini, and Athanasios V. Vasilakos (Hrsg.). *Energy Management in Wireless Cellular and Ad-hoc Networks*, volume 50 of *Studies in Systems, Decision and Control*. Springer, 2016.

[9] Prachee Singh, Yatindra Kumar Srivastava, Rahul, and Shelja Sharma. Ad hoc network based android messaging apps. *Department of Computer Science & Engineering, Galgotias College of Engineering & Technology and School of Engineering & Technology, Sharda University*, pages 1249–1253, 2013.

[10] J. H. Song, V. W. S. Wong, and V. C. M. Leung. Efficient on-demand routing for mobile ad hoc wireless access networks. *IEEE Journal on Selected Areas in Communications*, 22(7):1374–1383, 2004.

4 Anhang

[1]

[1] [3], [10], [5], [9], [8], [7], [2], [4], [1]